AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS FOR FISCAL YEAR 2006

WEDNESDAY, APRIL 20, 2005

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:30 a.m., in room SD–124, Dirksen Senate Office Building, Hon. Judd Gregg (chairman) presiding.

Present: Senators Gregg, Domenici, Craig, Allard, Byrd, Leahy, Kohl, Murray, and Feinstein.

DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF MICHAEL CHERTOFF, SECRETARY

OPENING STATEMENT OF SENATOR JUDD GREGG

Senator GREGG. I call the hearing to order.

Senator Byrd is the ranking member on this committee, and obviously on the full committee, and he will be here a little later. And when he arrives we will accord him the opportunity of making an opening statement if he should so wish.

We appreciate Secretary Chertoff coming here today. He's just assumed one of the priority responsibilities in our government relative to the safety of Americans. He's given up an extremely important position to take this position on, and it reflects well on him and I think on this administration as somebody who has caliber and is willing to do this type of a job, and we appreciate it.

However, the agency he takes over has some very serious problems, and this morning before this hearing I was just writing down—and I didn't do this with any staff assistance—just off the top of my head, the problems that I've seen and been reported to me over my brief tenure as chairman of this committee, they include things like the border patrol, the fact that our borders are not effectively protected anymore, that they are not—we have virtually no security along our borders, that people are pouring over the borders illegally.

It's gotten so bad that in Arizona citizen groups are now seeking to enforce the borders, which obviously is not good, that the border patrol training capabilities are not up to what the Congress asked them to be. We asked for 200 agents a year to be trained. Maybe they can do 400, 500, if they are fortunate. They cannot find people. They cannot hire them.

IMMIGRATION

In the area of immigration, this is an agency which has had a very long history of very significant management issues. Back when I chaired the Subcommittee on Commerce, State, and Justice before this Department was moved over to DHS; the Department had a lot of problems.

Even under the prior administration, the problems were significant and they have continued in the area of management. I don't think any member of Congress receives complaints about any agency with more consistency than about the immigration issues that we get.

IT ISSUES

We have got the issues of IT. The inability of the fingerprint capability at the borders to communicate effectively and in real-time with the database of the FBI. IDENT is not integrated into IAFIS.

We have the US VISIT program, which I have serious reservations about whether it is going where it is supposed to be going as a technology capability.

TSA

We have the TSA. It has become almost a weekly event now that there is some report that comes out about the TSA's failures in a variety of areas, from waste and fraud in the most recent IG report relative to the construction of its facilities for its headquarters to an internal investigation which I guess concluded that weapons and contraband were still going through the airports with regularity, which was totally unacceptable, to what I consider to be an inexcusable situation of a large amount of theft being reported from passengers in this country.

The fact that an agency of the Federal Government would have thousands upon thousands of reported thefts occurring by Federal employees against American citizens makes us look like a third-world country. And it still goes on.

Workman Compensation claims are outrageous. And I think anybody who goes through airport security has to ask themselves, at least occasionally when going through airport security, is this really having an effect on security or is this simply mindless when you see some of the actions taken by the TSA.

INTELLIGENCE

The intelligence issue, the agency has ceded intelligence over to other agencies when originally it was supposed to be the center of basically coordinating of intelligence. And now we see that the intelligence decisions are being made outside the agency by a conscious decision. And maybe it was the right decision, but essentially the IAIP has been raided the last 2 years from its resources to do other things. And I view intelligence as probably the essence of whether or not we win this war.

This is not a war about reacting to events. It is a war about getting to those events before they occur. And that involves intelligence.

PERSONNEL CONCERNS

The personnel issues, the senior management turnover is extraordinary. The number of people in an acting position is unacceptable and the number of positions which are unfilled at senior management levels is unacceptable.

ELECTRONIC SURVEILLANCE ALONG THE BORDER

The electronic surveillance capability along the border is non-existent right now from all I can tell. There has been a total breakdown in the camera structures; and the unmanned vehicle program has basically been stopped, even though it was proving very successful.

OTHER CONCERNS

Contingent to the agency's responsibility is the issue of protecting us against a biological or chemical attack. And granted, the HHS has priority here, but the Department has a very significant role in making sure that HHS is successful. And it is very obvious that in the area of vaccines, Bioshield has not produced the results it should have produced, and that we have not created a robust vaccine capability in this country against very significant disease issues, specifically anthrax, botulism, plague, and small pox.

Container ships, we all know we are not getting anywhere near the scrutiny on the container ships. If we look at the agency objectively, just on that list you have to say that were this agency admitted to an emergency room, it would be considered to be in extreme distress.

The fact is we have not been attacked. And credit on that goes to the Department, and I give them credit for that. But the fact also is there are very serious, serious problems, especially on what I consider to be the three core elements of the Homeland Security portfolio, which is protecting us from weapons of mass destruction attack, protecting our borders, and making sure that they are under control, and making sure that we have adequate intelligence capability.

So the problems exist now. You did not create them, Mr. Secretary. They did not come on your watch. You have just arrived. I congratulate you for setting up a Department-wide review of what is going on and trying to figure out how to correct it. But they exist and we have to get our arms around them.

FISCAL YEAR 2006 BUDGET REQUEST

The budget that has been sent up by this Administration presumes that the Congress will pass a significant increase on the fees of people who are flying. I do not think you are going to see this Congress accomplish that. Certainly, the chairman of the Commerce Committee here in the Senate has been more than vociferous in opposition to that proposal, and that is his authorizing committee, although this appropriating committee will play a role.

But if you take that number out, the budget that was sent up is well over a billion dollars less than last year's budget to operate this Department. If you put that number in, and giving you the benefit of the doubt that we are going to raise the fees on travelers

in this country by dramatic amounts, even though the stated amount is that the budget is up by 7 percent, our estimate is that the budget is up by about a $100 million.

Now it may not be that money solves this problem. In fact, I do not think it does. I think a lot of this is an issue of management and structure. But we know, for example, in the area of border patrol that getting more bodies on the border is critical, and that is going to cost money. And there are other areas where we know money may make a difference, for example, backlogs.

So I am not sure the budget that has been sent up is reflective of the urgency of the problem that this Department has relative to different functions that in my opinion are in distress.

So I hate to start this hearing off with a dark cloud, but I think honesty is required, and these are not reports which I have manufactured. They are restatements of public information.

So with that, again, I want to emphasize that I feel that we are extremely fortunate that you have been willing to take this job on. But I think you have been dealt a hand that is difficult to play, and I am looking forward to working with you to try to improve that hand. And that is the purpose of this committee, to constructively work with you to give you the resources you need to accomplish the improvements so that a year from now we do not have this long list of concerns. With that, we will listen to your thoughts.

STATEMENT OF MICHAEL CHERTOFF

Secretary CHERTOFF. Well, thank you, Mr. Chairman. And thank you for welcoming me to this first appearance for this subcommittee, which I am looking forward to working with as we go forward to improve our performance and make sure we are on the right track to, as you point out, protecting the American people, and protecting our infrastructure. And then if worse comes to worse, appropriately responding.

If I may, I would like to ask that the subcommittee receive my full statement for the record.

Senator GREGG. Of course.

Secretary CHERTOFF. I am going to be very brief so that I can be available to answer questions. Let me try in just a couple of moments to give you at high altitude the approach that I think we are taking in this review we have got going, and also in terms of our moving forward with the Department.

Quite obviously, in creating the Department, Congress wanted to do more than assemble 22 organizations in a tent. We wanted to create a single organization that could achieve outcomes that are important in terms of enhancing our national security. So one of the critical tasks I think I have as I begin my tenure at the Department is to see what we need to do in order to further the process of integration.

I completely agree that means intelligence, which is the driving guide to what we do all across the board. And we need to make sure we are appropriately collecting and fusing the intelligence we have available within the Department, and then contributing that to the community at large and consuming what the community has, and operationalizing that.

So we are looking to enhance our ability across the Department to combine our intelligence, combine our operations, and combine our policymaking. So we have a Department-wide approach to these things.

Second, as part of the review we are undertaking, I really want to be focused on outcome, and to kind of boil the jargon away. The example I have given to people when I try to explain what I mean, if my car is not running and I take it into the shop, and the electrician and the guy who does the transmission and everybody else takes a whack at it, and I come in at the end of the day to pick the car up, and everybody says, wow, you know, we have each done our process exactly right, but the car does not run, I do not consider myself a satisfied customer.

I am concerned about the outcome. I want a car that runs. And that is true here, too. We want a Department that produces the outcomes we care about, and we ought to focus on how we do that without regard to everybody's individual stove pipes. And then the alignment of the stove pipes and the alignment of the organizations and the operations has to be what fits with getting the outcomes.

The third piece is, we do want to use this risk-management philosophy. I think you pointed out, Mr. Chairman, in your statement, there are a lot of important things, but there are some things that are the highest priority. WMD is one example. And we have to be disciplined, since we are talking about a long-term issue with terrorism and threat, about identifying the priorities and figuring out how we go about optimally taking what are obviously finite resources and getting them to where they have to be. And so that risk management approach is going to be our guiding philosophy.

We are not interested in the Department of Homeland Security as simply an opportunity for people to, you know, raid the pots of money. We are interested in making sure that we get the money and everything we do over our deployment and our operations in a risk management, focused manner.

PREPARED STATEMENT

So with these kind of general observations, again, I am delighted to work with the subcommittee. I know it is a very challenging position, but I know there is a tremendous amount of support with the American public to getting this job done right. And that is what I am going to do my level best to do, and I look forward to answering questions.

Senator GREGG. Thank you. Thank you, Mr. Secretary.

[The statement follows:]

PREPARED STATEMENT OF MICHAEL CHERTOFF

INTRODUCTION

Mr. Chairman, Senator Byrd, and Members of the Subcommittee: Thank you for the opportunity to address you today, and for your ongoing support of the Department of Homeland Security's efforts to keep America secure and free. I am honored and pleased to appear before the Senate Appropriations Committee, Subcommittee on Homeland Security. This is my first appearance before this Subcommittee, and I look forward to a productive exchange as the Department begins to reassess and readjust priorities and policies in accordance with the changing threat of terrorism over three and a half years after the September 11, 2001 attacks.

For more than 2 years now, the Department of Homeland Security has led a national effort to protect our country and our citizens from all manner of threats. It has been an honor to join the dedicated men and women who carry out this task daily. Ours is a difficult mission—to prevent another deadly and catastrophic terrorist attack such as the one we experienced on September 11, and if an attack occurs, to respond quickly and prevent further damage.

The 180,000-plus people of the Department carry out this mission with unflinching resolve and a driving determination that such an attack should never occur on American soil again. Realizing that we can make no guarantees, we pursue our mission with a sense of urgency and daily diligence, so that this Nation can respond and recover quickly, should an incident or attack occur.

Since its establishment just over 2 years ago, DHS has made great strides in its efforts to unify the defense of our homeland. We have continued to integrate 22 distinct agencies and bureaus, each with its own employees, mission and culture.

But our security requires even greater coordination and effort throughout the Department, across all levels of government, and throughout our Nation to create synergy and new capabilities. It requires an unwillingness to accept complacency as part of anything we do; rather, we know we must apply all effort to tear down stovepipes and coordinate key intelligence, policy, and operational issues across DHS and the government.

SECOND STAGE REVIEW

I have therefore initiated a comprehensive review of the organization, operations and policies of the Department as a whole. This comprehensive review will examine what we are doing and what we need to do without regard to component structures and programmatic categories.

We want to understand better what's working and what isn't. We will be evaluating every element of our working mission and making sure that the Department is best organized to meet the threats—both current and future—that face our Nation.

Old categories, old jurisdictions, old turf will not define our objectives or the measure of our achievements because bureaucratic structures and categories exist to serve our mission, not to drive it.

Deputy Secretary Michael Jackson has been charged with overseeing this process. The goal of the review is to help me make informed decisions as I lead the Department. Deputy Secretary Jackson has selected a team of Department officials to look at a number of critical cross-cutting issues and determine how departmental resources and programs can be most effectively applied to achieve our security goals. I have asked them to get back to me by Memorial Day with the bulk of their recommendations. I intend to study and act on their recommendations.

What will the review cover? Take an issue such as maritime cargo security, which cuts across several departmental components. Customs and Border Protection, Coast Guard, Science and Technology, and Information Analysis and Infrastructure Protection each address aspects of this overall mission. Each might perform its element well, but we must go further to ensure that each is performing seamlessly and in coordination with the others, that we eliminate any duplication of effort, and that we reap the full strength of our wide spectrum of capabilities.

Of course, in executing the initial phase of putting the Department together and integrating the different components into a working structure, my predecessor and the men and women of Homeland Security did a tremendous job. They should be commended.

Now, as we enter into the second phase of the Department's life, we must also take a fresh, creative look at the Department itself—including its organization, its operations, and its policies. We are not yet fully integrated and our entities are still not always coordinated with each other. Now the challenge is to take the advantage of 2 years' experience and evaluate the Department to see if there are potential structural and operational changes that will improve and enhance our capabilities to protect and safeguard this Nation.

CROSS-CUTTING FUNCTIONS AND INTEGRATION

On the most basic level, we need to take a step back and focus on the fundamental question: Why was the Department of Homeland Security created? It was not created merely to bring together different agencies under a single tent. It was created to enable these agencies to secure the homeland through joint, coordinated action. Our challenge is to realize that goal to the greatest extent possible.

Let me tell you about three areas where I plan to focus our efforts to achieve that goal. First, we need to operate under a common picture of the threats that we are

facing. Second, we need to respond actively to these threats with the appropriate policies. Third, we need to execute our various component operations in a unified manner so that when we assess the intelligence and we have decided upon the proper policies, we can carry out our mission in a way that is coordinated across the board.

My intent is to integrate each of these three areas—intelligence, policy, and operations—across the Department, so that each is directed from the most senior level of the Department.

Let me turn to intelligence. Intelligence plays a pivotal role in mapping our mission. When the Department was created, 22 separate and distinct entities were woven together, a number of which had components focused on intelligence-gathering and analysis. One of my top priorities is to make sure that these various intelligence components function as a cohesive unit, and that our information and analysis is coordinated across the Department so that DHS, as a full member, can enhance its contribution to the Intelligence Community.

First, we must organize and combine all intelligence within DHS. To do this effectively, we must ensure that our own intelligence components are interoperable. The Department has already made progress in this area. For example, the Homeland Security Operations Center was stood up to help the Department develop a common operating picture and facilitate information sharing.

We must make sure that we are gathering all relevant information from the field, communicating with each other, and approaching analysis with a mission-oriented focus. We must ask, for example, whether those who evaluate the border from the Customs and Border Protection perspective are learning from analysts in the U.S. Coast Guard. They each look at border security, but from different vantage points. Only if they are working together can they fill in key gaps, paint a realistic picture, and evaluate all of the different pieces of information and intelligence that they are each gathering. We have to maximize the fact that all of these components now exist under the same umbrella.

Second, we must make sure that information is being disseminated both up and down the ranks of the Department. Strong and effective coordination does not just mean that our analysts at DHS headquarters are working together. We need to fuse and exploit all the information that we learn across the country, so that when a Border Patrol agent in Texas learns of a new alien smuggling method, that information is fed up to our intelligence analysts, incorporated where appropriate into our strategy to combat smuggling, and disseminated across the Department to others focused on the same problem. We must build a culture in which the disparate pieces of information are being transmitted to our analysts so that they, who have the benefit of the fuller picture, can properly analyze all of our information and inform our decision-making.

The converse must be true when our intelligence analysts learn of new vulnerabilities that terrorists are trying to exploit. That same agent in Texas needs to know, on a timely basis, of the threat and what he should be looking out for. We have a great many talented individuals at the Department. Some gather and analyze intelligence. Others learn critical information as they are in the field performing their jobs. The opportunities are endless. DHS needs to bring all of these nuggets of information together and disseminate them appropriately. We need to have the structure and the correct systems and technologies in place to take full advantage of them.

Third, our focus must extend beyond the Department itself. We must review and make use of intelligence coming from the Intelligence Community and we must play an active role in providing intelligence information to the Intelligence Community. As the WMD Commission made clear in its report 2 weeks ago, sharing information across the Federal Government is critical if we are to succeed. To that end, I am committed to making sure that our law enforcement and intelligence partners across the Federal Government have appropriate access to the Department's information and analysis, to the maximum extent possible under the law, while protecting the privacy rights and civil liberties of Americans. By the same token, we must sit as full partners at the table with full access to others in the Intelligence Community. We must work in concert with the Intelligence Community. I will work closely with the Director of National Intelligence, whose job it will be to make sure that the Intelligence Community is well-coordinated and mission-focused.

In addition, intelligence and information from other Federal agencies is critical to our efforts to secure the homeland. The development of the terrorism information sharing environment, as called for under the Intelligence Reform and Terrorism Prevention Act, will connect the resources (people, systems, databases, and information) of Federal, State, and local governments, and the private sector allowing users to share information and improve collaboration.

Finally, we must inform and communicate with our State, local, tribal entities, and private sector partners. As I observed just last week during TOPOFF, when it comes to securing the Nation, we must ensure that these entities are well-equipped both to react to crisis and to prevent it. As part of this effort, we must improve our ability to operationalize intelligence. As information comes in, we need to make sure it is getting out to the right people and in a way that they can use to strengthen their efforts and contribute effectively to ours. Intelligence in a vacuum is meaningless. We need to explain how our outside partners can counter that threat and what we need them to do to watch out for it.

Now, let me address policy development. Development and coordination of policy are major responsibilities of this Department. The Department has the central mission of securing the homeland, but there are many different aspects of that mission with numerous contributors. Large elements of DHS include traditional operational functions in which we deploy personnel, equipment, planes, ships and vehicles. But other elements principally involve planning and rule making, and networking with State, local, and tribal entities, and private parties. All of these must serve and promote our homeland security imperatives.

Therefore, we need to further enhance our capability to think through broad and overarching issues like border security, emergency preparedness, transportation security, and cargo security, with a Department-wide perspective, rather than just through the lenses of one particular component. We need to develop our policies by first looking at our missions and asking the comprehensive, result-oriented questions, rather than by looking to one particular entity that has the lead in driving an issue to conclusion.

Accordingly, I believe that we should pull together the vast expertise and the varying perspectives already at the Department as we work toward integrating our many crosscutting functions. For this reason, one of the areas that we are closely studying in the Second Stage Review is the advisability of creating a department-wide, substantial policy office. This office will also be a very important focal point for coordinating DHS's policy work with other Federal, State, local, and tribal entities.

Finally, let me discuss operational coordination. Just as with intelligence and policy, we need to find new ways to increase our operational coordination. Diverse operational components were woven together when Congress stood up the Department, each with its own history and identity. As I have become acquainted with these various components, I have quickly learned that there is a great deal of talent within them. Each entity has its own unique focus, but often they address the same mission from differing perspectives. But we cannot function as a cohesive unit, unless each operational component works together in combination to promote common missions.

This means that our operations must be driven by mission-oriented plans. It can no longer be the case that different components tackle different problems each in its own way and then later look to see if the pieces fit together. Whether it is preventing a potential act of terrorism, emergency preparedness, border protection, or countering a particular threat, we must first define the mission and second deploy all the tools within the Department to effectively execute each operation.

The Department has already begun this process. To take but one example, on the Arizona border, we have a cross-cutting initiative to protect the border, integrating intelligence gathering, border enforcement, and monitoring. It encompasses the efforts of several of our agencies, including Customs and Border Protection, Immigration and Customs Enforcement, Science and Technology, the Coast Guard, and Information Analysis and Infrastructure Protection. Each plays an integral role. The operations themselves involve patrolling the border, generating information, and using it to take enforcement actions. The genius of the Department of Homeland Security is that we have the capability within one department to do all of these things. But we need to carry out joint operational activities and have a joint perspective on a routine basis, not only when we stand up a special project.

Operations are also the mechanisms by which we respond to crisis. We cannot wait for a crisis, however, to learn, for example, whether TSA has the capability to communicate effectively and coordinate with FEMA. Nor can we learn in crisis that both are conducting the same operations or sending different messages to the private sector. The Department has made significant progress in this area. For example, it developed the National Response Plan to more effectively map out how to handle crisis situations. Now is the time to organize around missions rather than old bureaucracies, work through all of these potential disconnects in our systems, and operate as one unified Department. But integrating ourselves cohesively is not enough.

RISK-BASED APPROACH

I have been saying, and you will continue to hear me say, that we need to adopt a riskbased approach in both our operations and our philosophy. America is dynamic. Our strength as Americans is the sum of every generation that has ever been born in or immigrated to this great land. Our wealth and livelihoods are advanced by the inspired ideas and innovation of our own people. We prosper through the vast opportunities that exist to interact with the global economic community.

Risk management is fundamental to managing the threat, while retaining our quality of life and living in freedom. Risk management must guide our decisionmaking as we examine how we can best organize to prevent, respond and recover from an attack. We need to be realistic in our prioritization. We must assess the full spectrum of threats and vulnerabilities.

We all live with a certain amount of risk. That means that we tolerate that something bad can happen; we adjust our lives based on probability; and we take reasonable precautions. So, too, we must manage risk at the homeland security level. That means developing plans and allocating resources in a way that balances security and freedom when calculating risks and implementing protections.

The most effective way, I believe, to apply this risk-based approach is by using the trio of threat, vulnerability, and consequence as a general model for assessing risk and deciding on the protective measures we undertake.

Here I inject a note of caution because the media and the public often focus principally on threats. Threats are important, but they should not be automatic instigators of action. A terrorist attack on the two-lane bridge down the street from my house is bad but has a relatively low consequence compared, to an attack on a major metropolitan multi-lane bridge. At the other end of the spectrum, even a remote threat to detonate a nuclear bomb is a high-level priority because of the catastrophic effect.

Each threat must be weighed, therefore, along with consequence and vulnerabilities. As consequence increases, we respond according to the nature and credibility of the threat and any existing state of vulnerabilities. Our strategy is, in essence, to manage risk in terms of these three variables—threat, vulnerability, consequence. We seek to prioritize according to these variables . . . to fashion a series of preventive and protective steps that increase security at multiple levels. We must examine the mission and work of all elements of DHS through this template of consequence, vulnerability and threat. Have we fully defined our missions? How far have we gone in carrying them out? What more needs to be done?

The Department is already working with State, local, and private sector partners to further refine the Interim National Preparedness Goal to aid the targeting of resources to where the risk is greatest. There is much that we are doing. DHS agencies, for example, have provided unprecedented level of funding and resources since 9/11 to State, local and private sector partners to protect and prepare America's communities and individual citizens. We continue to improve the ways for first responders across the Nation to be better equipped, better trained and more capable of communicating across the public safety community. But we must bring even greater focus and discipline to our preparedness mission. We need to take a very substantive look at how we align our preparedness activities and functions. We need to look at how best to configure our organizations, operations, programs and policies so that we can think strategically about preparedness.

What should drive our intelligence, policies, operations, and preparedness plans and the way we are organized is the strategic matrix of threat, vulnerability and consequence. And so, we'll be looking at everything through that prism and adjusting structure, operations and policies to execute this strategy.

FISCAL YEAR 2005 ACCOMPLISHMENTS

Before beginning to outline the major themes of the Department's fiscal year 2006 Budget request, I would like to highlight a few of the Department's accomplishments over the past year, including the following:

—The Department established "the One-Stop-Shop" for first responder grants which allows a single point of entry to the Federal Government for homeland security preparedness resources.

—DHS has provided unprecedented levels of funding and resources to State, local and private sector partners to protect and prepare America's communities and individual citizens. We continue to improve ways for first responders across the Nation to be better equipped, better trained and more capable of communicating across the public safety community.

—U.S. Citizenship & Immigration Services (USCIS) is on track to eliminate the backlog of immigration benefit applications by the end of fiscal year 2006. In

fiscal year 2004, the agency increased productivity by 21 percent and successfully reduced the backlog to 1.3 million cases—down from a high of 3.8 million cases in January 2004.

—United States-Visitor and Immigrant Status Indicator Technology (US VISIT) was successfully implemented at 115 U.S. international airports and 14 seaports and immediately demonstrated results by preventing individuals with criminal records and immigration violations from entering the United States. In addition, US VISIT successfully deployed initial capability to the 50 busiest land border ports of entry in December 2004 and was also deployed at pre-clearance airports in Canada, Bermuda, the Caribbean and Guam.

—The U.S. Coast Guard (USCG) developed, reviewed, and approved 9,000 domestic vessel security plans; 3,200 domestic facility plans; 48 Area Maritime Security Plans and Committees; and verified security plan implementation on 8,100 foreign vessels.

—USCG interdicted nearly 11,000 undocumented migrants attempting to enter the country illegally by sea, saved the lives of nearly 5,500 mariners in distress and responded to more than 32,000 calls for rescue assistance.

—Counterdrug efforts remain a top priority for the Department. With the passage of the December 2004 Intelligence and Reform Bill, the Department's Office of Counternarcotics Enforcement is heavily invested in ensuring counterdrug operations and policy are synchronized across the Department, and that our components are adequately resourced to perform their counterdrug mission. In fiscal year 2004, the Coast Guard, Immigration and Customs Enforcement, and Customs and Border Protection collectively kept 489,870 pounds of cocaine from reaching the streets of our Nation.

—In support of Operation Iraqi Freedom the USCG protected, safely secured, and escorted to sea over 200 military sealift departures at ten different major U.S. seaports, carrying over 25 million square feet of indispensable cargo.

—The Homeland Security Operations Center (HSOC) Homeland Security Information Network (HSIN) infrastructure to facilitate providing Secret level connectivity has been expanded to state level Emergency Operations Centers in all 50 States, territories, and the District of Columbia.

—The Department's Information Sharing and Collaboration Office (ISCO) is responsible for producing immediate, near-term and long-term improved information sharing processes and systems. ISCO successfully partnered with DOJ to establish a first ever capability to share information between systems supporting law enforcement users across the country. The Homeland Security Information Network (HSIN), Regional Information Sharing System (RISS), Law Enforcement On-line (LEO), and Criminal Information Sharing Alliance Network (CISANet) now share information posted on each system with the users of the other systems with the result that over 7,000 documents are already posted and the numbers are growing every day. Users are able to access information on any of the four systems through a single sign-on, thus eliminating the need to access all four network simultaneously.

—Working closely with importers, carriers, brokers, freight forwarders and others, Customs and Border Protection (CBP) has developed the Customs-Trade Partnership Against Terrorism (C–TPAT) program, which has become the largest government/private partnership to arise from September 11.

—In carrying out its agricultural mission, Customs and Border Protection (CBP) Agricultural Specialist conducted 3,559,403 cargo inspections, 111,416,656 passenger inspections and made more than 400,000 interceptions of prohibited meat and animal by-products. During the same time period, CBP agricultural specialists intercepted more than 96,000 prohibited plant materials and found more than 64,000 agricultural pests.

—The Federal Emergency Management Agency (FEMA) provided $4.9 billion in aid, including hurricane relief efforts for victims and communities affected by disasters. FEMA, with its DHS counterparts, responded to 65 major disaster declarations and seven emergencies in fiscal year 2004.

—Passenger screening by the Transportation Security Administration (TSA) kept 6,501,193 prohibited items from coming on board aircraft during fiscal year 2004.

—In 2004, TSA screened approximately 600 million checked bags using advanced explosive detection technologies and over 31 million mail parcels using explosive detection canine teams.

—Since establishment of the Federal Flight Deck Officer (FFDO) Program in February 2003, TSA has selected, trained, and armed thousands of volunteer flight crewmembers to defend the flight decks of commercial passenger and cargo aircraft against acts of criminal violence or air piracy. To date, hundreds of thou-

sands of flights have been protected by one or more FFDOs serving in mission status.

—A total of 428 million people, including 262 million aliens, were processed at land, air and sea ports of entry. Of that number 643,000 aliens were deemed inadmissible under U.S. law.

—Immigration and Customs Enforcement (ICE) officers achieved a 112 percent increase over the prior year for fugitive apprehensions resulting in more than 7,200 arrests. ICE removed more than 150,000 aliens in 2004.

—Border Patrol agents apprehended almost 1.2 million illegal aliens between our official ports of entry.

—The Container Security Initiative (CSI), which involves pre-screening shipping containers to detect and interdict terrorists' weapons and other illegal material, was expanded to include 21 countries. CSI is now operational in 34 foreign ports in Europe, Asia, and Africa.

—Approximately 600 million checked bags were screened using advanced explosive technologies in 2004.

—More than 2,500 criminal investigations were conducted involving the illegal export of U.S. arms and strategic technology, including Weapons of Mass Destruction (WMD).

—The Federal Law Enforcement Training Center (FLETC) provided basic and advanced law enforcement training to more than 44,750 students, representing 81 Federal agencies, as well as State, local and international law enforcement organizations.

—Border and Transportation Security (BTS) assumed responsibility for visa policy under the Homeland Security Act and implemented improvements in visa review times and transparency.

—The Department planned, designed, and implemented security for five events designated as National Security Special Events (State of Union Address, G–8 Economic Summit, Former President Ronald Reagan Funeral, Democratic National Convention and Republican National Convention) as well as the support, integration, and coordination of hundreds of national special events not meeting the National Security Special Events designation.

—USSS arrested 30 individuals involved in global cyber organized crime, domestically and internationally. Industry experts estimate that $1 billion in total fraud loss was prevented.

—The Science and Technology (S&T) Directorate has implemented initiatives in chemical, biological, radiological, nuclear, and explosive (CBRNE) countermeasures, cargo security, border and transportation security, interoperability, standards for emergency responders, and cyber security. These initiatives have resulted in improved security of U.S. borders, transportation systems and critical infrastructure, and resulted in the greater preparedness of our Nation. To date, Department officials have visited more than 200 chemical, petrochemical, water, energy, (i.e. electricity, oil, liquefied natural gas, pipelines, storage, etc.) agriculture, commercial assets, national icons, soft targets, and mass transportation centers.

—The Department established the National Cyber Response Coordination Group (NCRCG) in partnership with the Department of Justice and the Department of Defense, as a forum of 13 principal agencies that coordinate intra-governmental and public/private preparedness operations to respond to and recover from largescale cyber attacks.

—The Department co-sponsored Blue Cascades II and Purple Crescent II, two regional tabletop cyber exercises in Seattle, WA and New Orleans, LA. Each exercise brought together more than 200 government and private sector officials to examine cyber security readiness and response procedures, highlight the importance of cyber security in critical infrastructure protection, and discuss solutions for integrating physical security and cyber security. Region-specific coordination and communication plans between first responders, the Federal Government, and critical infrastructure owners/operators were exercised.

—The Department established the US–CERT Control Systems Center to bring together government, industry, and academia to reduce vulnerabilities, respond to threats, and foster public/private collaboration to improve the security of the data and process control systems that operate our Nation's critical infrastructures.

—The Department established the Control Systems Security and Test Center (CSSTC) in conjunction with Idaho National Environmental and Engineering Laboratory, to provide an opportunity for government and industry to collaborate on cyber vulnerability enumeration and reduction activities for control systems currently in use across critical infrastructure sectors. The CSSTC models

map the cause and effect relationships of cyber attacks on control systems, assess the outcomes of actual events in a simulated environment, and provide the US–CERT with response and mitigation actions to share with partners in the control systems community.

—DHS and the Germany Ministry of the Interior jointly hosted a Multilateral Cyber Security Conference in Berlin, Germany. The conference brought together cyber security policymakers, managers from computer security incident response teams with national responsibility, and law enforcement representatives responsible for cyber crime from 15 countries. The conference program included a facilitated tabletop exercise and interactive discussions on how to develop an international framework—as well as near term actionable steps—for watch, warning, and incident response.

—The Information Analysis and Infrastructure Protection (IAIP) Directorate has developed and disseminated warning products (i.e. warning messages) to Federal, State, territorial, tribal, local, private sector, and international partners to protect citizens, governments, critical infrastructure, and key assets.

—IAIP has produced more than 70 "Common Vulnerability" reports executed over 250 Site Assistance Visits, nearly 600 Buffer Zone Protection Plans, and is continuing to build the National Asset Database. As of today, more than 80,000 "assets" have been compiled.

—Uninterrupted communications are critical for national security and emergency preparedness personnel in responding to a crisis. The National Communications System (NCS) issued an additional 17,000 calling cards, further enabling priority wire line phone communications and an additional 8,000 cell phones for priority wireless communications. In past disasters and crises, these capabilities have proved crucial.

—Pursuant to Homeland Security Presidential Directive-7, IAIP is coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States and has distributed the Interim National Infrastructure Protection Plan (Interim NIPP) to other Federal departments and agencies, the State Homeland Security Advisors, and the private sector stakeholder groups (e.g., the Homeland Security Advisory Council, Sector Coordinating Council, ISAC Councils, National Infrastructure Advisory Council, the U.S. Chamber of Commerce, etc.) The Interim NIPP provides a risk management framework for integrating and coordinating the Nation's infrastructure protection activities that takes into account threats, vulnerabilities, and consequences to manage a broad range of risks across the Nation's 17 critical infrastructure sectors.

—These important DHS activities were analyzed where appropriate for their impacts on personal privacy and civil liberties.

FISCAL YEAR 2006 BUDGET REQUEST

The Department's fiscal year 2006 Budget request revolves around five major themes: Revolutionizing the Borders; Strengthening Law Enforcement; Improving National Preparedness and Response; Leveraging Technology; and Creating a 21st Century Department.

REVOLUTIONIZING THE BORDERS

September 11, 2001 demonstrated the sobering reality that the United States is no longer immune from catastrophic attack. No longer do vast oceans and friendly neighbors provide the buffer against aggressive adversaries. In order to maximize the security of our Nation against persons determined to undermine the economy of the United States, our way of life and the freedoms we enjoy, the Department is determined to deter, thwart, and remove any threat to the Nation long before it reaches our borders. During fiscal year 2005, we will continue to strengthen our border security. For fiscal year 2006, the President's Budget includes several initiatives aimed at revolutionizing the Borders.

Weapons of Mass Destruction (WMD) Detection Technology is an integral part of the Domestic Nuclear Detection Office (DNDO) that includes a comprehensive strategy to address the threat of nuclear and radiological terrorism. The Budget includes $125 million to purchase additional Radiation Portal Monitors (RPMs) and pilot advanced next generation RPMs to detect both gamma and neutron radiation at our borders. In addition, the Container Security Initiative (CSI), which focuses on prescreening cargo before it reaches our shores, will have a preventative and deterrent effect on the use of global containerized shipping of WMD and other terrorist equipment. Egypt, Chile, India, the Philippines, Venezuela, the Bahamas and Honduras have been identified as expansion locations for this initiative in fiscal year 2006. An

increase of $5.4 million over fiscal year 2005 is included in Customs and Border Protection (CBP) budget for CSI. The total amount in the President's Budget for CSI is $138.8 million.

CBP's America's Shield Initiative (ASI) enhances electronic surveillance capabilities along the Northern and Southern land borders of the United States by improving the sensor and video surveillance equipment deployed to guard against the entry of illegal aliens, terrorists, WMDs and contraband into the United States. The Budget includes $51.1 million for ASI, an increase of $19.8 million. With additional technology investments, the President's Budget proposes to increase Border Patrol staffing over current levels to backfill staff vacated along the Southwest border, as well as increase staffing levels assigned to coastal areas. Since September 11, 2001, some Border Patrol agents were shifted to the Northern border in order to increase the number of agents assigned there. An increase of 210 positions and $36.9 million is included in the Budget for the Border Patrol. This increases the number of Border Patrol Agents to 10,949.

The Customs Trade Partnership Against Terrorism (C–TPAT), which began in November 2001, is another essential cargo security effort. C–TPAT focuses on partnerships along the entire supply chain, from the factory floor to foreign vendors to land borders and seaports. The President's Budget includes an increase of $8.2 million for this effort, bringing total funding for C–TPAT to $54.3 million. These funds will be used to enhance our ability to conduct additional supply chain security validations.

In addition to enhancing secure trade programs, the President's Budget also seeks to support additional investments in CBP's National Targeting System. CBP Targeting Systems aid in identifying high-risk cargo and passengers. The Budget includes a total of $28.3 million for these system initiatives, of which $5.4 million is an increase over the fiscal year 2005 level. Further, US VISIT, which will be consolidated within the Screening Coordination Office, will increase from $340 million to $390 million in the Budget. The increase will provide for the accelerated deployment of US VISIT at the land border and enhanced access for border personnel to immigration, criminal and terrorist information.

The President's 2006 Budget includes $966 million for the Integrated Deepwater System (IDS) to help address the Coast Guard's declining readiness trends and to transform the Coast Guard with enhanced capabilities to meet current and future mandates through system-wide recapitalization and modernization of Coast Guard cutters, aircraft, and associated sub-systems. Among other things, the IDS request funds production of the third Maritime Security Cutter-Large and continues HH–65 helicopter re-engineering to eliminate safety and reliability issues in the Coast Guard's operational fleet of short range helicopters.

Finally, within CBP, Long Range Radar technology is used by the Office of Air and Marine Operations to detect and intercept aircraft attempting to avoid detection while entering the U.S. CBP and the Department of Defense will assume responsibility for operating and maintaining these systems from the Federal Aviation Administration (FAA) beginning in fiscal year 2006. CBP's share is $44.2 million in the Budget.

STRENGTHENING LAW ENFORCEMENT

Law enforcement is a critical element in preventing terrorism across the Nation. Whether at the Federal, State, or local level, law enforcement agencies perform this vigilant task. As we know from unfortunate first hand experience, the known threats are creative, clever, and sophisticated. The Department's law enforcement agencies need to stay ahead of the threat. To achieve this, the Budget includes funding for numerous key initiatives to maintain and strengthen current law enforcement initiatives both within and beyond our borders.

The United States Coast Guard (USCG) is the Nation's leading maritime law enforcement agency. The President's Budget seeks additional investment in USCG assets to enhance its ability to carry out its mission. The President's budget provides $11 million to increase port presence and Liquefied Petroleum Natural Gas (LNG) transport security, funding additional Response Boat-Smalls and associated crews to increase presence for patrolling critical infrastructure, enforce security zones, and perform high interest vessel escorts in strategic ports throughout the Nation. This initiative also provides additional boat crews and screening personnel at key LNG hubs such as Baltimore, MD and Providence, RI to enhance LNG tanker and waterside security.

In addition, in the President's Budget, the Armed Helicopter for Homeland Security Project increases by $17.4 million. These funds will provide equipment and aircraft modifications to establish armed helicopter capability at five USCG Air Sta-

tions. This will provide the USCG and DHS with the tools needed to respond quickly and forcefully to emergency maritime threats. A total of $19.9 million is included in the Budget for this project. Finally, the Response Boat-Medium Project increases by $10 million the effort to replace the USCG's 41-foot utility boats and other large non-standard boats with assets more capable of meeting all of the USCG's multi-mission operational requirements. A total of $22 million is proposed in the Budget for this effort.

U.S. Immigration and Customs Enforcement (ICE), the largest investigative arm of the Department of Homeland Security (DHS), is responsible for identifying and shutting down vulnerabilities in the Nation's border, economic, transportation and infrastructure security. The President's Budget seeks a 13.5 percent budget increase for ICE, including increasing the Detention and Removal program by $176 million. For the Temporary Worker program, the Budget seeks to more than double the resources available for worksite enforcement including employer audits, investigations of possible violations and criminal case presentations. An increase of $18 million is proposed in the Budget for this effort. The President's Budget seeks a total of $688.9 million for ICE's Federal Air Marshal Service. This funding will allow ICE to protect air security and promote public confidence in our Nation's civil aviation system.

The Department's fiscal year 2006 Budget includes several other funding enhancements for law enforcement, including:

—The Federal Law Enforcement Training Center's (FLETC) budget increases by $2.7 million for Simulator Training Technology to teach officers and agents how to avoid collisions and reduce the dangers associated with pursuit driving.

—Federal Flight Deck Officers (FFDO)/Crew Member Self-Defense (CMSD) Training is increased by $11 million in fiscal year 2006. This allows for the expansion of the semi-annual firearm re-qualification program for FFDO personnel and to fund the first full year of the CMSD training program. A total of $36.3 million is included for FFDO/CMSD in the Budget.

—Enhancing law enforcement training through co-location of the Coast Guard's Maritime Law Enforcement Training program with the Federal Law Enforcement Training Center, increasing maritime law enforcement training throughput and promoting better coordination among field activities with other Federal, State, and local agencies.

IMPROVING NATIONAL PREPAREDNESS AND RESPONSE

Though the primary mission is to protect the Nation from terrorism, the Department's responsibilities are diverse. No DHS effort has a greater scope, reach and impact upon the citizens across the United States than our efforts to prepare the Nation to respond to major acts of terror or natural disaster. This Budget continues to support the President's homeland security directives that establish the methods and means by which our Nation prepares for and responds to critical incidents. Since its establishment, the Department has, and continues to provide, an unprecedented level of financial support to the State, local, and tribal governments and to certain private sector entities. The Budget builds on these efforts and proposes significant resources to provide direct financial assistance to our Nation's first responders, emergency managers, and citizen volunteers. There are several initiatives in the Budget geared towards improving national preparedness and response.

The fiscal year 2006 budget continues to support the Nation's first responders and seeks a total of $3.6 billion to support first-responder terrorism preparedness grants, administered by the Office of State and Local Government Coordination and Preparedness, with better targeting to high-threat areas facing the greatest risk and vulnerability. This funding will support State and local agencies as they equip, train, exercise, and assess preparedness for major emergencies, especially acts of terrorism. While there may be gaps in State and local capabilities, we believe special emphasis must be given to communications interoperability, catastrophic planning, WMD awareness, critical infrastructure protection, and cross-jurisdictional/regional cooperation and interaction.

For fiscal year 2006, the President's Budget proposes $20 million for the Federal Emergency Management Agency's (FEMA) enhanced catastrophic disaster planning. This funding will support catastrophic incident response and recovery planning and exercises. FEMA will work with States and localities, as well as other Federal agencies to develop and implement plans that will improve the ability of Federal, State, or local governments to respond to and to recover from catastrophic disasters quickly and effectively. FEMA will address the unique challenges a catastrophic disaster situation poses, including food and shelter, transportation, decontamination and long term housing needs.

On October 1, 2004, the Department of Homeland Security launched the Office of Interoperability and Compatibility designed to help State and local public safety practitioners improve communications interoperability. The Office of Interoperability and Compatibility (OIC), part of the Science & Technology directorate, oversees the wide range of public safety interoperability programs and efforts currently spread across Homeland Security. These programs address critical interoperability issues relating to public safety and emergency response, including communications, equipment, training, and other areas as needs are identified. The OIC allows the Department to expand its leadership role in interoperable communications that could be used by every first responder agency in the country. The OIC has currently identified three program areas: Communications, Equipment, and Training. With $20.5 million in fiscal year 2006, the OIC will plan and begin to establish the training and equipment programs, as well as continue existing communication interoperability efforts through the SAFECOM Program.

The President's fiscal year 2006 Budget for the Department proposes other enhancements to improve our national preparedness and response, including:

—Replacement of the USCG's High Frequency (HF) Communications System. Funded at $10 million in the Budget, this system will replace unserviceable, shore-side, high power high frequency transmitters, significantly improving longrange maritime safety and security communications.

—The Budget increases Cyber Security to enhance the U.S. Computer Emergency Preparedness Team (US–CERT), a 24/7 cyber threat watch, warning, and response capability that would identify emerging threats and vulnerabilities and coordinate responses to major cyber security incidents. An increase of $5 million is proposed, bringing the program total to $73.3 million.

—The Rescue 21 project is funded at $101 million in the Budget to continue recapitalizing the Coast Guard's coastal zone communications network. This funding will complete system infrastructure and network installations in 11 regions and begin development of regional designs for the remaining 14 regions.

LEVERAGING TECHNOLOGY

Rapid advances in technological capability are allowing the Department personnel to protect the homeland more efficiently and effectively across many components. To prepare the Nation to counter any WMD threat—threats from CBRNE substances—this Budget includes an increase for new initiatives that support research and development to counter these weapons and their potentially devastating effects.

First, the Domestic Nuclear Detection Office (DNDO) is being established as a joint national office to protect the Nation from radiological and nuclear threats. This office will consolidate functions within DHS and establish strong interagency linkages for the deployment of a national domestic nuclear detection architecture, the conduct of transformational research and development (R&D), and the establishment of protocols and training for the end users of equipment developed and deployed through the new office. The DNDO will integrate domestic nuclear detection efforts undertaken by individual Federal agencies, State and local governments, and the private sector and be closely linked with international nuclear detection efforts. A total of $227.3 million is requested for this effort in fiscal year 2006.

Second, TSA's emerging checkpoint technology is enhanced by $43.7 million in fiscal year 2006 to direct additional resources to improve checkpoint explosives screening. This request responds to the 9/11 Commission Report's finding that investments in technology may be the most powerful way to improve screening effectiveness and priority should be given to explosive detection at airport checkpoints for higher risk passengers immediately. This new equipment assures that TSA is on the cutting edge, ahead of the development of increasingly well-disguised prohibited items. This proposed increase will result in investing more than $100 million in fiscal year 2005 and fiscal year 2006 for new technology to ensure improved screening of all higher risk passengers.

In addition, to improve TSA's information technology network, the President's Budget includes $174 million to complete installation of High Speed Operational Connectivity (Hi–SOC) to passenger and baggage screening checkpoints to improve management of screening system performance. Within the Screening and Coordination Office, funding is sought for the Secure Flight and Crew Vetting programs—an increase of $49 million to field the system developed and tested in fiscal year 2005. The funds will support testing information systems, connectivity to airlines and screen systems and daily operations. This also includes an increase of $3.3 million for crew vetting.

Third, the President's Budget also proposes additional funding for two critical Department programs—the Homeland Secure Data Network (HSDN) and the Home-

land Security Operations Center (HSOC). For fiscal year 2006, the Budget includes $37 million for HSDN. This funding will streamline and modernize the classified data capabilities in order to facilitate high quality and high value classified data communication and collaboration. Funding for the HSOC is increased by $26.3 million, bringing its fiscal year 2006 funded level to $61.1 million. This includes an increase of $13.4 million for the Homeland Security Information Network (HSIN) and an increase of $12.9 million to enhance HSOC systems and operations. The funding will provide the HSOC with critical tools for sharing both classified and unclassified information and situational awareness with Federal, State, local and tribal governments.

Fourth, a key element of the Department's Maritime Security Strategy is to enhance Maritime Domain Awareness (MDA), leveraging technology to improve sharing of accurate information, intelligence, and knowledge of vessels, cargo, crews and passengers, mitigating threats to the security, safety, economy, or environment of the United States. The fiscal year 2006 budget funds several key MDA initiatives, including $29.1 million for the nationwide Automatic Identification System (AIS) and $16.5 million to provide additional maritime patrol aircraft flight hours in support of detection, surveillance and tracking activities.

Finally, the Department is seeking additional technology investments in other critical areas, such as:

—$20 million for developing a Low Volatility Agent Warning. This system will serve as the basis for a warning and identification capability against a set of chemical agents whose vapor pressure is too low to be detected by conventional measures;

—Increasing Counter-Man Portable Air Defense Systems funding by $49 million to a total of $110 million in the Budget. This program will continue to promote the viability of technical countermeasures for commercial aircraft against the threat of shoulder-fired missiles by improving reliability and affordability.

CREATING A 21ST CENTURY DEPARTMENT

The Department has made significant progress in strengthening the management of its business processes from inception to implementation. The Office of the Under Secretary for Management focuses its efforts on the oversight, integration and optimization of the Department's human capital, information technology, financial management, procurement and administrative operations. Over the past year, this office has made strides in designing, planning, and supporting new standards for business processes and resource allocation in order to achieve a cohesive organization while ensuring maximum return on investment. This organization is focused on establishing the overall framework, developing management methods, and monitoring the progress of each management function.

Examples of major enterprise initiatives included in the Budget that contribute to Creating A 21st Century Department include the following:

—The program for electronically managing enterprise resources for government effectiveness and efficiency—or eMerge2—to continue implementation of a DHS-wide solution that delivers accurate, relevant and timely resource management information to decision makers. The Budget includes $30 million for this program. By delivering access to critical information across all components, the Department will be able to better support its many front-line activities. It focuses on the areas of accounting and reporting, acquisition and grants management, cost and revenue performance management, asset management and budget that will be integrated with MAX HR.

—MAX HR funding of $53 million involves designing and deploying a new human resources system. The $53 million is requested to support the development and deployment of the new HR personnel system as published in the Federal Register on February 1, 2005. These funds will be used to fund the detailed system design for our labor relations and pay-for-performance programs, provide appropriate training and communication for our managers and employees and to provide proper program evaluation and oversight. In this effort, our goal is to create a 21st Century personnel system that is flexible and contemporary while preserving basic civil service principles and the merit system.

—The Information Sharing and Collaboration (ISC) program will affect the policy, procedures, technical, business processes, cultural, and organizational aspects of information sharing and collaboration, including coordinating ISC policy with other Federal agencies, drafting technical and operational needs statements, performing policy assessments, and analyzing new requirements. The total funding for fiscal year 2006 will be $16.482 million.

These initiatives will help move the Department toward an efficient and effective shared services environment, avoiding duplication of effort across the program areas.

CONCLUSION

Two years ago, Congress and the President took on the enormous undertaking of creating a new Department whose central mission would be to secure the homeland. Under Secretary Ridge's leadership, the entities that now comprise the Department of Homeland Security unified under this overarching goal. As I have become acquainted with the many talented people of the Department, I am impressed by all that they have accomplished thus far. But there is no time to pat ourselves on the back.

As the Department initiates our second stage review, organizes around missions, eliminates duplications, and adopts a risk-based approach, we must identify our crosscutting functions and ensure that we are thinking innovatively how to best exploit our intelligence capabilities, develop policy functions, execute our operational tasks, and implement our long-range preparedness planning.

I thank the Congress for its support, which has been critical in bringing us to this point. I am grateful to be here today to talk about the work we are doing to make America a safer home for us, for our children and generations to come. Thank you for inviting me to appear before you today. I look forward to answering your questions.

NUMBER OF BORDER PATROL AGENTS NEEDED

Senator GREGG. It is hard to know exactly where to begin, because there are a lot of issues here. But let me begin with some of the higher priority items as I see them. And I congratulate you on the risk management approach. I think threat is the issue to finding threat and then responding to it.

Clearly, one of the priority issues from the standpoint of threat is who is coming into the country and where they are when they get here, and who they are when they come across. There have been a whole lot of amendments floated this week on expanding the number of border patrol agents. I actually asked the folks down at border patrol if they had an assessment as to how many agents they needed and where they needed them, and I was told that, no, they did not.

I found that to be a startling fact, in the sense that I would have presumed that there has been a study done within the last 2 years as to where the agents are needed and to what numbers are needed. Obviously, there has been a significant movement of agents to the northern border.

I guess my question is: How many border patrol agents do we need and where do we need them——

Secretary CHERTOFF. Well, again——

Senator GREGG [continuing]. In comparison to where we are today? Congress has, as you know, required an increase of agents by 2,000 each year for a 5-year period.

Secretary CHERTOFF. I know that in the Intelligence Reform Act authorizations were put in place for 2,000, going forward. The President's 2006 budget looks for an increase of slightly more than 200.

I can tell you, because I have sat with Border Patrol, that we do have a comprehensive picture of where we need to deploy our resources. We had an Arizona Border Control Initiative last year, which was successful. This year, I guess about a month ago, we rolled out a follow-up to that initiative, and in talking with Commissioner Bonner and the other leaders of the Border Patrol about

how to do that, they took a very unified approach to figuring out where the sectors of the border where we are now seeing the greatest penetration.

How do we deploy not only Border Patrol at the front line, but technology, and also a capability to transport people that we apprehend and bring them back in a way that does not pull people off the line in order to drive them several hours back to Tucson.

How do we use checkpoints? How do we use investigative resources to target organizations? And also, frankly, how do we work with the Mexicans on their side of the border to see that they are doing things to attack these human trafficking organizations.

So I do think that we have a comprehensive plan about dealing with the issue of deploying resources in a unified——

TRAINING OF BORDER PATROL AGENTS

Senator GREGG. But is 2,000 the right number, a year? And can you train—how many people can you train—let us say we actually funded 2,000, which clearly we are not going to do, but we are going to significantly increase the funding. In fact, Senator Byrd has a proposal to do that, which I presume he is going to offer within the next day or so, and increase border patrol agents.

STATUS OF TECHNOLOGY IN USE ON THE BORDERS AND DETENTION SPACE

How many agents can you train? And two, what's the status of the unmanned vehicle program and did it work? And if it did work, why is the line basically being shut down? And three, what's the status of the electronic surveillance in the cameras? And four, how many detention beds do we need? We hear about a lot of people being sent home who are criminals and who should probably be detained permanently here to make sure they do not come back to commit further criminal acts? How short are we on the detention bed area?

Secretary CHERTOFF. I might forget all this, so if I do, I mean to come back. I'll give you the answer. With respect to training, obviously, the President's budget talks about 210. We can certainly train and assimilate that. I do not know that this is the limiting number in training, but I would also be inclined to agree, I doubt we could train 2,000 even if one had 2,000.

Certainly, we can train and deploy the 210 that we have asked for on top of whatever we are replacing in terms of attrition.

The UAV program, as I understand, did work well. We are currently working now to begin the process of procuring UAVs. We would like to get that done in a matter of months and start to put UAVs up and have them flying over the border.

Now I don't think we can rely exclusively on UAVs. I think that sometimes you need manned vehicles and you need helicopters. But I think it was generally viewed as a positive program, and we are in the process of getting the RFIs and RFPs out in order to make sure that that gets done.

As far as detention beds are concerned, again, the budget contemplates adding some additional beds. I do want, I guess, to address an issue which seems to come up a lot when we talk about releasing people. The fact of the matter is, we do not detain every

single illegal person that we apprehend. And frankly, I have to say, as a graduate of the criminal justice system, neither does the criminal justice system.

Most people who are arrested in States all over the country get released on bond. What everybody does, whether they are criminal justice people or people in the immigration areas, is prioritize. And I do think we are working very hard to make sure that the people who are mandatory detainees are being detained and that we have adequate beds to do that.

ELECTRONIC SURVEILLANCE

Senator GREGG. And the camera situation that allows electronic surveillance on the borders?

Secretary CHERTOFF. I beg your pardon?

Senator GREGG. The camera situation relative to electronic surveillance. I mean there was a contract let that appears did not work and now I guess they are trying again. What is the status on it?

Secretary CHERTOFF. I gather, and I think this is under investigation, there was a contract let and there were some problems with the procurement process. This goes back a number of years. The procurement phase of that contract is over. Obviously, we are maintaining.

My understanding is that as a general rule the surveillance stuff does work well. Obviously, we have maintenance issues. We are now going to begin the second stage of that, which is the America Shield Initiative, where we are sending out RFIs and RFPs to begin the process of acquiring technology.

Obviously, we are going to learn something from the procurement problems in the last round that go back several years, but again, it is a very good technology. I mean the idea of using cameras and remote sensors does work. As long as we get, you know, the right contractor and the right equipment, and it is handled in a cost-effective manner, I think that is a very promising way to go about handling it.

Senator GREGG. Well, maybe you could have your staff tell us whether or not—we know we had the wrong contract. We spent a lot of money.

Secretary CHERTOFF. Right.

Senator GREGG. We bought cameras that did not work. Supposedly, this has been corrected. We would like to get some specifics on that.

Secretary CHERTOFF. We will get back to you on it.

[The information follows:]

BACKGROUND ON GSA BASIC PURCHASING AGREEMENT WITH IMC

The Remote Video Surveillance project was formed in 1998 to install camera systems mounted on poles or towers near the U.S. Border. These cameras would transmit video images back to a control room where a Law Enforcement Control Agent (LECA) could view the images and dispatch Border Patrol agents as necessary.

The Immigration and Naturalization Service's Office of Information Resource Management (OIRM) managed the RVS program. From its beginning, the OIRM faced tremendous pressure to get RVS poles installed or face losing their funding. At first, the OIRM administered the RVS Project through a series of individual purchase orders with various contractors. OIRM would give bills of material (BOMB) to NTMI, a GSA FAST contractor, for the equipment needed for the installations.

NTMI would procure the equipment and store it until needed for an installation. Chugash was the contractor used to install the poles, cameras and monitors. IMC was the contractor used to install the microwave transmission equipment.

A competition was conducted in 1999 in order to increase accountability for the installations and to obtain volume discounts for the equipment involved. GSA considered four companies for this award: the three listed above and Hazmed, a contractor that has assisted OIRM in managing the purchase orders for the other three contractors and that had core competencies in the area of installing electronics systems. IMC was selected as the contractor in March 1999 and given an initial task valued at $2 Million.

In November of 2000, in an effort to optimize procurement procedures, OIRM and GSA agreed to convert the GSA schedule award to a Blanket Purchasing Agreement (BPA). The rationale for the BPA was that it would "further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive individual purchases from the Schedule contract."[1] The end result was to "create a purchasing mechanism for the Government that works better and costs less."[2] The hope was that the reduction of costs would allow for funds to accelerate deployment of additional RVS systems.

Installation of RVS sites was completed in three phases. The first phase involved administrative preparation (i.e., environmental assessments, rights of entry (ROE), real estate issues, permits, and survey activities). Phase I activities generally required between 16 and 18 months to complete. However, there were often issues with access to the land desired for the surveillance site, or environmental assessments, which caused greater delays.

The second phase of the installation involved groundbreaking activities such as installing foundations and poles, assembling and populating platforms, installing power, aligning equipment and radios, and installing equipment shelters. This phase took between 3 and 6 months.

The third and final phase lasted approximately 1 month. It involved installation of the cameras, transmission lines, consoles, other related electronics and the build out of control rooms. Finally, after completing build out of the control room and successful integration testing, the Border Patrol agents would begin using the RVS system. The timeframe for an average RVS installation varied between 20 and 25 months. $239 Million was allocated to GSA for the RVS BPA. Approximately $220 Million was expended by the contractor during its term, which ended on September 30, 2004. At that time there were 248 completed RVS sites. Since that time, six more sites have become operational for a total of 254 sites. The Border Patrol is working with GSA and the contractor to finalize the credits due back to the government for incomplete installations.

Currently the Headquarters Office of Border Patrol's Integrated Project Team is seeking contractor support to complete the installation of 21 Phase III RVS sites partially installed by L–3 Communications Corporation. Government furnished equipment bought under the terms of the BPA will be used to complete the 21 sites. The Headquarters Office of Border Patrol projects these 21 sites will be completed by the end of calendar year 2005.

Senator GREGG. I think I have certainly used up my time, although this clock does not seem to be working correctly.

But in any event, Senator Byrd, did you want to make an opening statement or pursue questions? It is—obviously, the floor is yours.

STATEMENT OF SENATOR ROBERT C. BYRD

Senator BYRD. Thank you. Thank you, Mr. Chairman.

And thank you, Mr. Secretary. Mr. Secretary, you and the 179,000 employees in your Department are to be commended for your efforts to preserve our freedoms and secure our homeland. I applaud Chairman Judd Gregg for taking on the challenge of chairing this subcommittee.

---

[1] The Immigration and Naturalization Service Integrated Surveillance Intelligence System (ISIS) Equipment and Services Blanket Purchase Agreement (BPA) between GSA Federal Technology Service (FTS/FAST) Region 5 and the International Microwave Corporation Team, GS05KR01BMC0001, dated November 8, 2000, page 2 of 12.

[2] Ibid.

His predecessor, Senator Thad Cochran, did a superlative job as chairman. Under Chairman Cochran, this subcommittee worked on a bipartisan basis to provide the Department of Homeland Security with resources to fill critical gaps in our security. Of course, you should know, and I am sure you do know, Mr. Secretary, that Chairman Gregg brings excellent credentials to this task.

As a former governor, he understands that simply setting a policy in Washington does not automatically make that policy a success. We have to work effectively with State and local governments and with the private sector to protect the homeland.

Years before the tragic events of September 11, Chairman Gregg led the way by funding State and local antiterrorism programs. He authored provisions for training and equipping first responders for chemical and biological attacks.

In fact, if you want to meet the father of the Office of Domestic Preparedness, the predecessor to your office of State and Local Government Coordination and Preparedness, I am sitting right next to him, on my left, today.

Mr. Chairman, I look forward to our partnership on this subcommittee, and I thank you for taking on this assignment.

I thank you, Mr. Secretary, also. As the Secretary of Homeland Security, you are responsible for a critical balancing act. We are a Nation that thrives on liberty, but 9/11 taught us that we also must invest in our security. I hope that you will work with the Congress to make sure as much as possible that your Department promotes our security without sacrificing our liberty.

I wrote to you on March 2 to express my dismay that the President's budget fails to fund the border security investments authorized by the Intelligence Reform and Terrorism Prevention Act of 2004 which he signed into law on December 17 of last year.

That Act authorizes the hiring of 2,000 new border patrol agents per year for 5 years, the hiring of an additional 800 immigration investigators per year for 5 years to enforce our immigration laws, and the funding of 8,000 new detention beds for the holding of illegal aliens.

BUDGET AMENDMENT

I urged you to work with the White House to propose a budget amendment seeking resources to increase security on our borders and to enforce our immigration laws. Despite the statements by Secretary of State Rice and former Homeland Security Deputy Secretary Loy that al Qaeda is a threat on our porous borders, there is virtually nothing in the President's budget to provide these additional resources for border security.

According to Former Deputy DHS Secretary James M. Loy, when testifying before the Senate Select Committee on Intelligence about threats to the United States, "Current intelligence strongly suggest that al Qaeda has considered using the southwest border to infiltrate the United States." According to Secretary of State Condoleezza Rice, "we are all concerned about terrorists and how they might use our very long and porous borders. The terrorists are going to keep trying. They're going to keep trying on our southern border. They're going to keep trying on our northern border."

So, I could not help but be disappointed to read your response to my letter yesterday that no budget amendment would be forthcoming.

The threat to our security is clear. The holes in our borders are well known. I look forward to hearing from you on this and other issues today. I thank you, and I thank you, Mr. Chairman. I thank all the Senators.

Senator GREGG. Thank you, Senator Byrd, and thank you for your generous comments. Did you wish to proceed with questions at this time?

Senator BYRD. Would you please have someone else go and then call on me at your leisure.

Senator GREGG. All right.

Well, then I think I would turn to Senator Feinstein, I believe, was the first member of your party here.

Senator BYRD. Very Well.

STATEMENT OF SENATOR DIANNE FEINSTEIN

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

I want to say, Judge Chertoff, that at least for this Senator you are so far a breath of fresh air, and I am delighted to say that. I just want to publicly thank you for your response of April 6 in the use of fraudulent passports, stolen or lost passports, which is a big problem.

I know that from the intelligence committee. And your letter was no-nonsense, and it set forward very directly what the Department is prepared to do. I, for one, will certainly hold you to it.

And I am very pleased that you share my concerns about the visa waiver program, and indicated, you know, that you share the findings of the critical reports that have been done, and that you have established a visa waiver program oversight unit. So I look forward to—my understanding is that you are probably going to come in asking for another extension on the visa waiver program.

My vote, as you know, is conditioned on getting the management act together in that unit, which critical reports have said has been in disrepair for some time. So I just wanted to say that.

BORDER PATROL

I want to follow up on what the chairman said on the border patrol. The expansion of the border patrol is not really just the recommendation of the 9/11 committee. Those of us on the judiciary committee have recommended this for a long, long time, and specifically, the border reform and visa entry law recommended an enhanced border.

As you know, 600 agents have retired this past year. So on a four-to-one basis, whether the 210 additional agents is actually going to provide you with a net gain or not, I think, is somewhat dubious, and I am really concerned about it. The position of the border patrol on 2,000 agents, going back 6 years, has always been they do not need them, they do not have the room to train them. I mean this goes on year after year after year. The time has come to fish or cut bait. That is no longer, I think, a justifiable response.

Bills have called for this. The President says he calls for it. Although, only 210 will not do it. I would like to get your real answer

to this, because on the southwest border, other than Mexican intrusions have gone from 22,000 in 2002 to 88,000 in 2004. This clearly indicates that the southwest border is being utilized as a point of major penetration into this country by other than Mexicans. If you look at the list of apprehensions made from countries that are terrorist States, there are numbers there as well.

So I have a hard time, in view of the Minutemen coming on the Arizona border, the remonstratives made by this Congress over and over and over again as to why there cannot be a net large increase in border control. This is something I think we are willing to pay for. This is something that I think we would be willing to add. And yet, year after year it is the same kind of 200, which does not make even for retirements. Could you respond, please?

VISA WAIVER

Secretary CHERTOFF. Well, first let me begin by just, if I can, for a moment go back to your visa waiver point. I mean as I think you indicated, Senator, I share your concern. We have to look at the border as a whole and make sure we are addressing every possible point of entry. And I certainly intend to hold the Department to what I have indicated to in the letter we need to do to make sure——

Senator FEINSTEIN. Thank you.

Secretary CHERTOFF [continuing]. Our end is up. And I have spoken to our foreign partners and talked about the importance and I have spoken personally to them about the importance of making sure they have their house in order in terms of tracking and getting us information on this, and ultimately moving to a biometric passport that is resistant to the kind of alteration or counterfeiting, which is obviously a vulnerability.

SOUTHWEST BORDER CONTROL

The southwest border, obviously, is a concern as well. As I understand it, what we are proposing to do in the budget is a net increase of 210 border patrol agents, which would fill those that are leaving and fund an additional 210.

Senator FEINSTEIN. So if I may, that means 810 new border agents?

Secretary CHERTOFF. I do not——

Senator FEINSTEIN. Six hundred have retired.

Secretary CHERTOFF. I think new. As I understand it, new means over and above what we currently have, the funding level we have. So that we will wind up at the end of the day with—and I cannot do the math in my head, but I guess there is approximately 10,800 currently. We would be adding about 200. That should include backfilling for positions that are becoming vacant. I mean that is keeping the funding level steady and then adding 210.

So that is what we contemplate, in addition to which we want to be able to bear the UAVs. As I told Chairman Gregg, we want to acquire those and start to put those up. I think that was a successful pilot program, no pun intended. And we do want to do more with sensors, which, again, notwithstanding the contracting issues, apparently, several years ago, we think the idea of the sensors and the usefulness of sensors is proven. So we have an America Shield

initiative and we are in the process of setting out RFIs in order to start acquiring that technology and deploying it.

This is obviously an issue that we have to constantly look at. I am going to go down to the border at some point in the next month or two. I want to see for myself how we are doing down there, and what additional things we can do. We have redeployed agents down to the Arizona border to deal with the issue of a surge of people coming across.

I totally agree with the principle that this is a paramount responsibility of ours, and I am going to be spending a lot of personal time focused on it.

Senator FEINSTEIN. Thank you. My time is up. Thank you.

Senator GREGG. Senator Craig.

STATEMENT OF SENATOR LARRY CRAIG

Senator CRAIG. Mr. Secretary, like all of us, let me welcome you to the committee, and let me also speak, as others have, about our belief that you are the person who can get the job done.

At the same time, let me not sound like a broken record, but let me repeat what has been said here by both our chairman, our ranking member, and certainly the Senator from California. I am going to focus on our southwestern border again.

Because I have been a bit outspoken about immigration policy and changes in it, and I actually led the Senate in debate for the last 2 days on it, I have also been given a lot of attention by those who might criticize any form of policy change, but most importantly, it has led to a lot of conversations about border. And it has allowed me to focus more intently on border. Because I will tell you, if we cannot control our border, we will never be able to write immigration policy that works. We will always be playing catch-up to an ever increasing number of illegals in our country.

The Senator from California and I have discussed this at length. Probably every one on this committee today has a slightly different opinion about how we handle the problem, but I think we are all in concert about how we handle the border.

So my folks in Idaho say build a fence high and build it strong, and spare no cost. Now there are a variety of ways to build the fence, and you're exploring all of them, but there are also not just the physicalnesses of it and all of the tools that we are going to acquire and should acquire to control that border.

There are other issues as to who is there and how they handle process and movement. We have got this interesting situation. Yuma, Arizona. A lot of folks live on the other side of the border, but work across in Yuma. They harvest lettuce. Your folks were out there a few weeks ago rounding them all up early in the morning to come back across the border, because many of them were undocumented illegals. But by 2 o'clock in the afternoon they were back in the fields harvesting the lettuce.

The crisis of the harvest was over, but the reality was that a great deal of border movement occurred during that day. And in that movement, there could have been someone that meant to do this country harm, not just to pluck lettuce from the fields of Yuma, Arizona. And that is something we have to get under control, both sides of that issue.

So let me give you a dialogue that I had with a young man who sought me out because of my position on this committee last year, a very frustrated member of the intelligence community. He and his group were prevented from apprehending suspects at the border because of strict guidelines and the chain of command, even though it was his group's responsibility to collect the intelligence.

His group had gathered immediate intelligence regarding certain aspects and actions needed to take immediate action. However, because of the chain of command and the hamstringing that resulted, certain intelligence agents, this intelligence officer had to sit and watch while suspects possibly crossed the border.

These were not Hispanics. These, by all appearances, were people of Arabic descent. They were believed to be terrorists. And yet the outcome still today is who is on first and who is second and who is in control. And in that fight, people are crossing our borders at an unprecedented rate.

And while we can talk about the money we have spent, and I did on the floor yesterday, billions of dollars, with a "B," and we apprehended a 1,750,000 or 1.2 million last year, or something like that. Big numbers. It demonstrates one thing when we are apprehending them, that they got across.

And I cannot imagine that when someone is illegal, by definition, and they are apprehended, that they are turned loose. At least take them to the border and shove them across. Do not say, "Well, they will come back." They do not come back.

All of us are going to be able to control this process, and I am going to keep pushing for changes in the law that are realistic and that work. But all of a sudden the Senator from California and I are engaged in conversation, and I say my proposal will affect 500,000 or 600,000 or 700,000, and she says, "No, it will not. It is millions."

I do not know whether she is right or I am right. We may both be right in some ways. But we do know there is a huge problem. Enough said.

I guess my question is: Go to the border. Look it over. Get to understand it. It is unique in a variety of ways. And lastly, I was in Houston, Texas, over the weekend. I was visiting with a former State judge, who said to me very directly, there is a clear understanding in Texas that the laws are not going to be enforced because they are unenforceable. And I am talking about border laws.

BORDER PROBLEMS

Now if that is the name of the game along the border, we have got a huge problem that you must get your hands around and get it under control. I agree with the Senator from West Virginia. I am a co-sponsor of his amendment to pull money in this emergency supplemental to give you more. Either build the fence or we do something that causes that border crossing to stop. How do we do it?

Secretary CHERTOFF. Well, first of all, Senator, there are a number of things you raise, and I hope I keep them in mind so I can address them all. I think it is important, as you say, to look at this as a comprehensive issue, not an issue you can deal with in terms of individual slices of policy.

TEMPORARY WORKER PROGRAM

Clearly, one piece of this is the issue of what the President has advocated addressing through a temporary worker program, finding a way to bring some portion of the people who come across the border not to do us harm, but to work, to bring them within the system.

Senator CRAIG. Very important.

STEPPED UP ENFORCEMENT ALONG THE BORDER

Secretary CHERTOFF [continuing]. So that we have some control over them, and also we then reduce the pressure and we reduce the demand which gives the trafficking organizations the kind of resources they need to bring bad people across the border. Now that is one piece of a comprehensive package. Another piece has to be stepped up, enforcement along the border, including better deployment and more efficient deployment of border patrol, use of technology to give us a better span of control over who is coming across the border.

Absolutely, the idea that there are laws that are tacitly not going to be enforced is dead wrong, and something certainly I do not endorse.

When you talk about chain of command issues interfering with somebody apprehending persons coming across illegally, I have to say, I mean if there are bureaucratic obstacles to enforce in the law, I want to get rid of those. I have spoken to Border Patrol and to Commissioner Bonner about, in fact, breaking down the stove pipes that I think used to be. We used to have very regionally controlled, border sector controlled deployment of resources so that you had seams between the regions. Everybody took the view that, hey, I am going to worry about my region and that is all I am going to worry about.

We have now moved away from that. Commissioner Bonner has put together a much more nimble program for deploying resources, which I think, again, is trying to break down those stove pipes. When I hear about these kinds of bureaucratic things, I do want to go out and see what the problem is and try to fix it.

This problem has been around for a long time. When I was U.S. attorney back in the early Nineties we were talking about this. So I know it is not a new problem. I know there is a new urgency. And I think although there is a lot to discuss in terms of detail, I think there is a general view we have to take a comprehensive approach. And I really look forward to working with you and with everybody who is interested in this in putting together a comprehensive policy.

Senator CRAIG. Thank you.

Senator GREGG. Thank you. Senator Murray.

STATEMENT OF SENATOR PATTY MURRAY

Senator MURRAY. Well, thank you very much, Mr. Chairman.

And, Mr. Secretary, thank you for being here today. You have been handed a very, very difficult job, and I commend Senator Gregg for his opening statement and agree we need an honest as-

sessment from you of what resources we need for all of these difficult challenges.

PORT SECURITY

I think everybody here shares the same goal of doing everything we can to make sure our country is secure and it is always difficult when we feel like we are not getting what we really need. We have heard a lot about border security. I obviously am concerned about the northern border. I know all 200 of those, plus, are going to the southern border. We know that the northern border is a problem, but let me set that aside, because I want to focus on port security and cargo security, which you and I have had some time to talk about.

I am very concerned. The Coast Guard commandant testified before us that it would take more than $7 billion to implement the Maritime Transportation Security Act. So far, Congress has provided a little over $500 million of that. I do not think any of that was requested by the Administration. That was Congress adding those dollars in.

Now for the past 2 years, about a billion dollars in port security grants have come in to your agency, and the American Association of Ports Authorities say they need at least $400 million to help secure port facilities this year.

From our discussions I know port security is an important issue for you. You understand it is not only human life. It is economic disaster if we do not secure our ports. But it is disconcerting to me that the Administration does not ask for the dollars for these port security grants.

Does the Agency just discount all the intelligence reports that tell us our ports are a significant risk, or what can we expect on this?

Secretary CHERTOFF. No. I mean I do think ports are a very significant part of the infrastructure we have to work to protect. One thing I want to emphasize: You know, as we go through this process of reviewing the entire operation of the Department over the next couple of months, I try to look at the issue, whether it be ports or rail or aviation, in terms of an outcome or an approach.

In other words, I don't want to know what each agency is doing. I want to know what we are doing in combination to deal with the issue of ports or rail or aviation, because that gives us our total sense of how good we are doing or how well we are doing in protecting ourselves.

There are a number of dimensions to this. First of all, there is container security. We have begun a container security initiative, which pushes our screening and inspection process overseas. That is a very positive——

Senator MURRAY. Well, I want to ask you about that separately in just a minute. What I want to ask you about first of all, is the port security—under the Maritime Transportation Security Act, our ports have to harden the ports, and they are just not getting the resources to do that.

Secretary CHERTOFF. We want to make sure they get adequate resources, bearing in mind, again, with the philosophy of risk management, that we have to prioritize.

Senator MURRAY. But the Administration is not requesting any money to do that, despite the fact that the commandant of the Coast Guard told us we needed $7 billion to do that.

Secretary CHERTOFF. Well, I do think we have money in various grant programs that are requested in the budget that are available to be used for purposes of strengthening ports. We have infrastructure, proposing an infrastructure protection program. We have State grants. We have urban assisted—UASI grants.

We have a lot of different kinds of types of grants, but I also have to say I think that the issue of how we protect the ports has to be looked at comprehensively. Coast Guard plays a role in that. Private parties play a role in that, and have——

Senator MURRAY. I understand that——

Secretary CHERTOFF [continuing]. Private obligations.

Senator MURRAY [continuing]. But under the Maritime Security Act we directed all of these ports to give us a plan of how they were going to protect their ports, which they did. And they now have to implement it. They are not getting any money to do it. And we need a direct targeted program, the Port Security Grant program, to do that.

So I want to work with you on that. I am just disappointed every time when the budget comes over with no money for that, because as you and I both know, a disaster at one of our ports is going to dramatically hurt not only human life, but the economy of this country, whether you are in a port city or not.

CARGO SECURITY

But the other part of that is cargo security. And as you know, I have been really pushing to get some kind of coordinated port security regime in place. Everyone out there is trying their best to move those ports out, to follow our cargo from where they are loaded, into our ports here, and there is no coordinated approach to that.

In the committee report from last year, we directed the Undersecretary of Border and Transportation Security to help us develop a plan for that coordinated approach. It was due February 8. We still have not gotten that yet. And I just feel like—we need the Administration—I have talked with you about this. I have talked with Commissioner Bonner. I have talked with a number of folks about it. And all we get is, "We're going to study this." I know that you and I agree this is an important issue.

How can we help you come up with a coordinated approach to secure our ports, all the cargo that moves through them, and the people who work and live there?

Secretary CHERTOFF. Of course, I am very sensitive to being—you know, not saying we are studying something. So let me be a little bit more concrete.

Senator MURRAY. Thank you.

Secretary CHERTOFF. We need to take the issue of cargo and container security to whatever is considered to be the next level of systems sophistication. There are people in the private world who are very, very good at tracking everything, from point of departure to point of arrival. And there are processes and technologies that

allow us to do that. And that is the kind of system we ought to be looking to moving toward in our container security initiative.

CSI is part way towards that. The principle of moving this overseas is a good step in that direction. We have been meeting with, for example, the private sector, and shipping companies, to talk about ways we might, with greater specificity, track cargo from the time that it departs the manufacturer to the time it gets to the point of arrival, working with the private sector to have them build a security envelope.

And again, through the C–TPAT program, we have got that process as a precedent. We do use that kind of process, so that eventually what we can do is put as much of the cargo through a security envelope from point of departure to point of arrival as possible, track it, screen it, have private sector take a lot of responsibility within that envelope for maintaining security, use technology to make sure we are not getting penetrations, and then, again, you are always going to have some cargo that does not fit within that envelope.

We are deploying technologies like VACAS radiation portal and our National Targeting Center to focus on that subset of cargo that really needs a much tougher regime of screening and inspection. So that, I think, this is the way forward. And I do think we are working with a lot of diligence and a lot of urgency to move into that next level.

PREPARED STATEMENT

Senator MURRAY. Well, I appreciate that. Mr. Chairman, it is a very complex problem. There are a lot of players in it, and what I think is most disconcerting to me is that we do not have a coordinated approach. Mr. Secretary, I hope we can get that report from you that was due February 8 so that we can really start moving forward to get that accomplished.

[The statement follows:]

PREPARED STATEMENT OF SENATOR PATTY MURRAY

Thank you Mr. Chairman. I want to join you, Senator Byrd, and the rest of our colleagues in welcoming Secretary Chertoff to the Committee.

Mr. Secretary, I want to thank you for taking the time to meet with me prior to your confirmation. We had a good discussion about many of the issues we are going to talk about today.

I know that you are still new to the job and understand that this budget request was formulated before you were nominated.

I also understand that you have been handed a tough task in a very difficult time. But from our private conversations, I know that you are committed to keeping our country safe—and I look forward to working with you.

That being said, I fear this Administration—through this budget request—is failing in this most important responsibility.

Mr. Secretary, as you are well aware, the Department you now lead faces enormous challenges.

Concerns that DHS is not meeting the Nation's security challenges are growing—in the Congress, and among the American public.

Don't get me wrong, in fact, I believe Secretary Ridge and Admiral Loy did the best they could with the hand they were dealt.

Merging so many complex entities into one organization was a monumental challenge. We all knew success wouldn't come overnight.

But many of DHS' problems were created by this Administration because it didn't request adequate funding.

Mr. Secretary, the Administration has many priorities—we all do.

The bottom line is that current White House fiscal policy isn't consistent with providing the resources DHS needs to provide the level of security the American people deserve.

To compound this problem, DHS has spent what funding has been available in a scattershot way. There appears to be very little rhyme or reason to how funding is allocated compared with actual threats.

And, we are hearing about it on a daily basis.

Just this morning, we're reading newspaper reports about financial mismanagement at TSA. I don't want to get into that now because I know you'll have an opportunity to respond this morning.

But please know that it just makes it harder for us in Congress to help DHS succeed.

Mr. Secretary, I want to work with you to ensure our budget will actually deliver the security we both seek for our country.

But if we are going to work together, we need to be honest about what resources are necessary to do your job and let the Congress worry about budget priorities.

For example, adding to what I believe is already an insufficient budget request, the Administration assumes user fees that we all recognize are not going to be approved.

In fact—$2 billion of the $2.5 billion increase in the Administration's request would come from a 60 percent increase in airline passenger fees.

Fees placed on the back of an industry that we all know is having significant financial difficulty.

Mr. Secretary, these "proposals"—if not accepted by the Committee—only make the funding problem worse.

As I'm sure you are aware, the Senate has included $276 million for Immigration and Customs Enforcement (ICE) in the Emergency Supplemental Appropriations bill.

This is funding that we all agree your agency desperately needs. In fact, many of us have known about this issue for quite some time.

Last year, I asked Commissioner Bonner and ICE Assistant Secretary Garcia about a news report highlighting a budget shortfall that would result in a hiring freeze at ICE.

At that time, I was told the problem was an accounting error resulting from combining budgets from legacy agencies.

Now it's clear that it was a real budget shortfall and the Senate was forced to include this as new money—designated as an emergency—to enable ICE to lift its hiring freeze.

Curiously, this money was not part of the Administration's supplemental funding request.

Mr. Secretary, the Senate's action speaks volumes about how much we want this agency to succeed, but we need the Administration's help.

We need realistic annual budget proposals—not reprogramming requests and not emergency supplemental requests.

Mr. Chairman, I don't say this to denigrate the performance of any of the hard working men and women who serve us so ably on the front line. Like Secretary Chertoff's predecessor, they are doing a tremendous job with the tools they are provided.

But, this Committee—and the Congress—must do a better job of providing oversight to this agency because right now we are failing the American public.

Mr. Secretary, I know that you, Chairman Gregg, Senator Byrd and the rest of our colleagues care about these issues as much as I do.

And, I don't want to dwell on this too much—but I think it is important context for the other specific issues that I'd like to discuss here today.

I'm quite concerned that good intentions are not going to help us:

—Establish a rigorous port and cargo security regime,

—Protect our borders, or

—Train our personnel correctly

Mr. Secretary, I look forward to your testimony, working with you to address these issues, and ensuring our budget will actually deliver the security we both seek for our country.

Thank you Mr. Chairman.

Senator GREGG. Thank you, Senator.

Senator Allard.

STATEMENT OF SENATOR WAYNE ALLARD

Senator ALLARD. Thank you, Mr. Chairman.

And I also would like to join my colleagues and welcome Secretary Chertoff here this morning. I am also new to the committee here, Mr. Secretary, and I am looking forward to serving under the able chairmanship of Senator Gray.

I wonder sometimes if maybe we are not looking too much to a Federal solution and perhaps should not think a little bit more about what the local law enforcement along the borders. That is the counties along the borders. It is the States along the borders.

This is homeland security. Everybody is talking about more money for Customs and more agents and whatnot, but I happen to believe that those people down along the border that form the Minutemen organization have some real concerns. I think they are really concerned about their property. I think they are really concerned about the safety of their families.

I do not know whether any thought has been in trying to do more to support our local law enforcement along the borders. They are local elected officials. They know about those things. They understand the problems of their community. I wonder if we should not do the same thing with the State. The governor is elected by that State.

I wonder if we should not consider targeting those counties, share with them more of the technology that we have developed at the Federal level, and take citizen groups, incorporate them. Deputize them. Have the local sheriff deputize them or whatever, or have your National Guard or whatever, bringing some responsibility.

I am not implying that they have not been responsible at this particular point in time, but at least bring them under some organized law enforcement thing that traditionally has relied on citizens. That is why we have deputization process. That is why we have the National Guard.

I wonder how much thought you have given to that, because all I am hearing from this committee and all I am hearing so far in this discussion is a Federal solution. I think we will get a better bang for the buck. I mean they are worth a lower salary level. They have more of a commitment in that safety because they live there. I wonder if you would comment on that.

Secretary CHERTOFF. Well, we do work, actually, in the Arizona border control initiative, we are working. We have had a great working relationship with State and local law enforcement officials now.

I guess depending on what community you are in, some law enforcement officials want to be involved and engaged in the process of enforcing the laws against illegal immigration. Some do not. I do not think we can make them do it.

Clearly, though, we want to work cooperatively, because they are a force multiplier. And when we get well trained and we share information, and we get well-trained State and local enforcement officials, they are a welcome addition to the process of extending our ability to deal with the issue of illegal migration across the border.

Senator ALLARD. Well, obviously, you have been in conversation with local elected officials. I just think we can do more. And I think I will be a voice on this committee, at least, for pushing you towards more of a local solution than something run out of Washington. I do not think we have all the answers necessarily here in Washington.

VISIT TO ONE OF THE PORTS

The other thing that I would like to say in a positive way is there has been a few million years since we have had a coastline in the State of Colorado. So I made a personal concerted effort to visit one of our ports. I visited the port of Miami. And I will have to tell you, I was pretty impressed.

And this is the very thing that you talked about in your previous testimony, I saw happening there. I saw technology developed at the Sandia Laboratories in New Mexico being used at that port. And I have to tell you that I feel much better about our port security.

And I think sometimes we are looking at a 100 percent solution. I do not think the citizens of this country can afford a 100 percent solution. But I think we have to come up with some reasonable solutions that work. And I think what I saw there at the port, it was efficient, where they could handle a fair amount. I saw a lot of dedication there, and I was really pleased. I just have to tell you that.

AIRPORT SECURITY

I think sometimes what we see happening in our airports, I wonder if maybe we have not gotten off track a little bit and expecting too much on security in airports. I think the most important thing we did and probably the most cost-effective thing is we put a door that was secure between the pilot and the passengers. But I do think that we need to take a hard look at what is happening at our airports to see if we cannot come up with some more commonsense solutions to what I see happening. So I think there are some good things happening there.

RUDENESS OF CUSTOMS EMPLOYEES

On the other hand, I have also seen, as I have walked through Customs, and particularly in the State of Colorado, and I have been appalled at the rudeness of the employees there. I come from a State where I want to welcome people to my State as tourists. And I have been sort of appalled at some of the rudeness that I saw at Customs.

So hopefully we can kind of improve our bedside manner a little bit. Remember that we have visitors coming to our country. We have visitors coming to our States.

Secretary CHERTOFF. And they are not all criminals.

Senator ALLARD. And if that—yes. And they are not all criminals. If the Federal employee does not treat them respectfully and with a welcome attitude, it hurts our tourism in our State. So I just want to call that to your attention.

Thank you, Mr. Chairman.

Senator GREGG. Senator Byrd.

STATUS QUO BUDGET REQUEST

Senator BYRD. In fiscal year 2004, Immigration and Customs Enforcement (ICE) removed a record 150,000 illegal aliens from this country. However, we know that more than 10 million illegal aliens reside in this country. Two and a half million illegal aliens have overstayed their tourist or work visas. There are over 370,000 illegal aliens who have knowingly disobeyed orders to leave the country.

ICE teams, Immigration and Customs Enforcement teams, deported 11,000 of them in 2004, but more than 35,000 others were added to the list. The system is not working, and this budget request does almost nothing to fix it.

I have a border security amendment pending to the Iraq war supplemental, which is currently being debated on the floor of the Senate. My amendment is offset, responds to known security shortfalls on our borders, and responds to the concerns of many Americans, including the self-styled Minutemen who are performing a major community watch effort on the Arizona border.

While there are, indeed, slight increases proposed for next year, the fact remains that both the Border Patrol and Immigration and Customs Enforcement are experiencing significant attrition this year. According to your agencies, 137 Border Patrol agents have left the service since the beginning of the fiscal year. By the end of January, ICE had experienced a net loss of 299 positions.

On average, you are filling 2,000 fewer detention beds a week than the level for which the Congress provided funds. The proposed increases for next year merely backfill the losses you are experiencing this year. In short, this is a status quo budget request.

The crisis we are experiencing today on our borders deserves more than a status quo budget. Why should we be satisfied with a status quo budget, Mr. Secretary?

Secretary CHERTOFF. Well, Senator, first of all, my understanding, again, of what we are proposing to do is that we are going to—when we talk about increases, we are talking about net increases. In other words, we are going to fund over 200 additional Border Patrol Agents, 140 additional ICE investigators, almost 2,000 additional beds over and above the current level.

Obviously, when people leave, we always backfill those positions, so that I think you have to add those numbers together. And we are talking about funding that would get us a net up-kick in all those categories.

In fact, in terms of 2005, we have submitted a reprogramming to get more money to ICE so that even this year we can begin the process of starting to do some hiring to move them to the level they need to be.

There is no question there is a serious issue, this whole issue of managing illegal immigration. What we have to do is use a comprehensive approach. We have to be able to have more people at the border, better technology at the border, all of which we are now pushing forward. Better investigative capability. Better and more available use of detention beds. And we are doing some additional things as well to free up beds.

REPATRIATION PROGRAM WITH MEXICANS

For example, we are working with the Mexicans to begin the internal repatriation program in the next couple of weeks, whereby we transport Mexicans who come in back to interior locations so that they do not simply go back across the border, connect up with the same trafficking organizations, and then come back a couple of days later.

EXPEDITED REMOVAL

We are using other kinds of techniques in terms of expedited removal to try to expedite the process of getting people that we do apprehend, moving them, again, across the border back to Mexico.

ABSCONDERS AND VIOLATORS OF RELEASE ORDERS AND RETURN ORDERS

We are now targeting for the first time enforcement of people who are absconders or who are violating release orders and return orders to make sure we are apprehending them, and we are, again, getting them and sending them back across the border. And we have to also be vigorous in enforcing the laws against people who are removed and then in violation of the law come back across the border again. We have not always succeeded in getting the kinds of sentences we need from judges in keeping those people who are violators, repeat violators in prison.

So we are very concerned about it. We are taking steps to move forward on this. I am going to look at this issue. As I said previously to Senator Feinstein, I am going to go down to the border, I think, within the next 2 months and talk myself personally to the local people and our Border Patrol folks down there to keep moving forward on this issue.

SATISFACTION WITH STATUS QUO BUDGET

Senator BYRD. Well, are you satisfied with the status quo budget?

Secretary CHERTOFF. I am not satisfied with the status quo. We need to move forward. We need to be better about keeping our borders policed. We need to be better about tracking absconders. We need to be better about getting people removed efficiently. And I think as we look at the whole issue comprehensively, there are a lot of things we can do to get a better outcome.

Senator BYRD. Mr. Secretary, you did not answer my question.

Secretary CHERTOFF. Well, I think what I——

Senator BYRD. Are you satisfied with the status quo budget?

Secretary CHERTOFF. I think what I am saying, Senator, is I think our budget is not a status quo budget. I think it looks to net increases, and, therefore, I will tell you, I would not be satisfied with a status quo budget or a status quo situation.

Senator BYRD. Finally, Mr. Chairman, we would look forward to your comprehensive approach. My amendment will provide you with real resources to implement your comprehensive approach.

Thank you, Mr. Chairman.

Senator GREGG. Senator Domenici.

STATEMENT OF SENATOR PETE V. DOMENICI

Senator DOMENICI. Thank you, Mr. Chairman.

Senator Byrd, I will follow up on your questions and give my own observation after first saying thank you for the job you are doing. I look forward to visiting the border with you and some of the facilities that we have in our State, such as the DOE laboratories, to make sure you understand the competence in other departments of the government to help you do your work.

Senator Byrd, I would say I laud your concern about doing more than we are doing, which is an answer to a status quo. We cannot stand the status quo. I do not know about a status quo budget. But we also cannot stand a status quo with reference to our current laws on migration and immigration.

I mean they are adding to the problem, because it is a mix-up and a mumble-jumble of things and agents do not know what they are supposed to do. I mean when we catch illegal aliens on this side and send them home, what are agents supposed to do when they come right back? I mean we did then look at it and say they are not doing their job.

Senator BYRD. I am with you.

Senator DOMENICI. It is embarrassing to see that we do not have a bill yet on the floor of the Senate on immigration. This is not a way to deal with immigration on a supplemental appropriation bill. I think you would agree with me. We need to debate this issue thoroughly, and it makes them do their job better and adds to the propriety of the United States.

Senator BYRD. I have been singing that song for many years now.

Senator DOMENICI. It is time. I am telling you, many of us agree with you, finally.

Senator BYRD. Thank you.

OBSERVATIONS REGARDING THE DEPARTMENT OF HOMELAND SECURITY

Senator DOMENCI. Now having said that, first, let me say to you, people wondered when you got this job what somebody with your background was doing. I was at your side all the way, because I know what you are capable of doing. I want to laud you so far with the job you are doing. I want to give you a couple of my observations.

First of all, you inherited a Department that was put together hurriedly. It is consequently a very hodgepodge Department. The sooner you yourself find out what was done that is not done right, what was done that might even be wrong, you ought to be the one finding out about those problems and fixing them, because they are going to be determined sooner or later. There are many of them up and down the chain of command of your Department, and you know that. I do not know how soon you can fix them, but I urge that you do so.

My second observation is: Since we put the Department together this way, there is a multiplicity of activities that are, even though we thought we are putting them all together, that they are not all together, because there are many other facilities that do work of the type you need.

I really urge that even though you have set up in the statute a function and thus a piece of your Department, that you resist your Department creating a total group of experts in every one of those niches. Because many of those experts already exist in the government, and you ought to use them. You are using them. I think you should just make that a policy.

Somebody said, this distinguished Senator from Colorado, who shames me, he has been to see Miami, and I have not been to the border in 6 months, which is my own State. He has been way over there in the port of Miami. I ought to go see what is happening on my border.

The problem is that in enforcing our laws, there exists terrific capacity in our national laboratories, in our Defense Department, and those who are studying unmanned aerial vehicles. You do not have to begin every program within your Department. Do I make sense?

Secretary CHERTOFF. Yes. Absolutely, Senator. I mean I really do not want to rediscover the wheel, particularly if we have the wheel discovered elsewhere in the Federal Government or the State government, and the private sector. I mean we do not have the time to do everything ourselves.

One of the observations I had when I came into the Department, two observations. One is completely consistent with your advice, that we really need to comprehensively review what we are doing. I give a lot of credit to Governor Ridge, and Admiral Loy and everybody who stood up in the Department, which was an enormous challenge. They did a lot in 2 years. It took the Defense Department decades to get to where it is now. And we do not have that time. So we should be willing to examine where we can adjust and make those adjustments.

With your second point, Senator, a lot of what we bring to the table is a network. Nowadays in business, people talk about networking. We do not have to own or employ everybody in Homeland Security. We do not and we cannot. What we have to do is network with what is out there in our other Federal agencies, State and local partners, and figure out a way to make everybody work together and to coordinate those things.

So even in my brief 2 months at the Department I have been very clear about saying that we ought to pay as much attention, if not more, to that networking function as we do to the actual physical assets that we own and the people that we have in our Department.

IMPACT OF NETWORKING

Senator DOMENICI. Well, my time is running out. I am going to make one last observation. I will put it two in one.

First, it seems to me, without question, that what you are doing out there in terms of networking is already having a big impact. I am not one who continues to carp on the fact that we do not have good homeland security, because I contend that nothing has happened since 9/11. And that is not an accident.

I think we are doing a much better job at making it hard for terrorists than we give ourselves credit for. Now I do not need you to answer that, but if you can, you should. I mean everybody is just saying we are not doing anything, but why are the terrorists doing

nothing? They keep saying they want to get America. They have not done anything yet. Thank God. Maybe tomorrow they will do it, and Domenici will be crazy. But that is one observation.

And the second one is that it seems to be obvious that even though we want to address risks, we nonetheless want money to go to the States. And the new bill will do what you suggest, and put more money in risks and less in pork projects, allegedly. But I submit that this does not mean that all the heavily populated States are the harbors of all the risks.

I mean in my State you have two national laboratories filled with nuclear activity, the center of nuclear weaponry. That is all I will say. You know what that means. Now you cannot expect New Mexico with .005 tenths of a percent of the money to assume the risk of the extraordinary activities.

I would hope that if we give you a law that does what I have just said, that you have somebody looking at West Virginia and New Hampshire and New Mexico to say what else is there that is essential to our country and dangerous. I do not mean a football field. That is what people are saying. Every gym and football field, because people will assemble, ought to be protected. I do not know about that. You decide that.

But I do know the place where nuclear weapons of the United States are in abundance shall not say, "Well, that's old New Mexico. It's a rural State." Do you understand what I am saying?

Secretary CHERTOFF. I absolutely do. As you have said, I think risk management is not about size of State or population or things of that. It is about individual pieces of infrastructure, individual networks of transportation. I mean population clearly is an element to be considered, but we have to have a much more sophisticated approach. And I think that is exactly what we want to drive to, is our risk management philosophy.

Senator DOMENICI. Thank you, Mr. Chairman.

Senator GREGG. Thank you. Senator Kohl, I appreciate your patience. Please take as much time as you think you need.

STATEMENT OF SENATOR HERB KOHL

Senator KOHL. Thank you, Senator Gregg and Secretary Chertoff.

I would like to talk about airport screening. For those of us, and it includes I assume most of the people here in this room, we are going through, as you know, a lot more intensive airport screening today than we were prior to 9/11. And yet a report came out this week which indicates that investigators have determined that things like knives, guns, and even fake bombs are still being processed through the screeners without detection.

It is almost incomprehensible. I am trying to figure how that can be after all of the money and the effort that we have put in to trying to improve airport security for travelers. They talk about the need for new technology, additional technology, which we apparently do not have or have not yet been able to spend the money on.

Can you tell us whether or not it is true that airport screening today is about at the level that it was before 9/11, and how soon it is that we are going to be able to improve it.

Secretary CHERTOFF. I read the IG's report and I just spoke with the IG about it, because obviously I was very concerned about that. I do not have an independent way of verifying it, but I am not going to dispute it either.

I was very concerned about the question of how do we move to the next level. Clearly, there are issues involving training and things of that sort, which are important, but I agree with the IG that technology is really ultimately what we have to use in order to get to the next level.

We do have some good pilot projects and we do have some good technology. We are continuing to fund that, and I think that is a very promising development. I have to be completely forthright in saying we also have to make some difficult decisions about policy in order to decide if we are going to capitalize on that technology.

BACKSCATTER TECHNOLOGY

For example, one form of technology that makes it easier to detect these kinds of threats is backscatter technology. That has certain implications for privacy, because it does essentially, in some form, allow you to look to see what someone is carrying on them that they may be concealing. And so there is sometimes resistance to that.

I think we have to be prepared to say that we need to start to deploy these kinds of technologies and make appropriate adjustments for privacy if we are going to get to that next level. The technology is out there and it is being used. It is a question of the decision to deploy it and to try to balance that with legitimate privacy concerns, but not get so caught up in an endless debate about it that in 5 years we are still sitting there with the technology available and useful and helpful, but we have not put it out yet because people are still hand wringing about it.

So I very much want to start to take the step of moving that technology out and continuing to press forward on the research and development side, but also not letting the perfect be the enemy of the good. If we can make things better, let us get them better rather than wait for the magic bullet that is going to solve everything.

IMPROVING AIRPORT SECURITY

Senator KOHL. Yes, it is very surprising to me and I think to every traveler to think that in spite of all the money that we spent and the delays that we now go through at airports that we did not go through prior to 9/11, some people in the position to know are saying that airport security is about at the same point that it was then. This, I am sure, is a matter of great concern to you, and I hope that we can effect some improvements.

Secretary CHERTOFF. Well, I intend to do so. It is troubling. I think we do have good capabilities in technology, and I think we have to now start to move the process forward. And I am very interested in seeing that we do that.

FOREIGN STUDENT VISAS

Senator KOHL. Okay. I would like to talk about foreign student visas for a minute. As you probably know, there has been a signifi-

cant increase in the time that it takes for foreign students to get their visas to enter this country to attend school. And as a result, the number of applications has gone down, the number of foreign students who are enrolling post-graduate has gone down. And universities all across the country are quite concerned about this.

In 2003, it was indicated that 40 leading research universities reported that 621 students missed the start of classes because of visa delays. Now certainly we need to do the job of checking out, keep out those students who should not be here for security reasons, but is there not something we can do to increase our level of ability to move people through the process and allow them to get enrolled in universities?

Secretary CHERTOFF. Well, we should. I have talked to Secretary Rice about this. We have already taken some steps in terms of lengthening the period of time a visa is applicable so that at least once we have passed someone through the screen they have an ability to spend more time without rechanneling themselves through the process. That is a positive development.

Obviously, we need to do more in terms of our ability to vet people in advance, to do it more quickly. And we need to also, frankly, send the message out that we want to be hospitable in doing those things. So I think we are all committed in moving that forward.

Again, I want to be fair and like I said be blunt in saying the schools also have to help, too, because we do encounter situations where people come in for schools and they do not show up or they leave the program. And, of course, we should know about that. The school should report that to us. And certain schools get a reputation as being easy marks for people who want to come and maybe not to study, but to do something else.

If the schools do not cooperate with us, they make it very hard to run the program in a way that helps the entire spectrum of universities. So part of what we need to do is make it more efficient for people to get their visas, give them longer visas, but also make sure the schools live up to their obligation to let us know if people are abusing the system. And that is part of the tradeoff in order to make this work for the best interest of everybody.

Senator KOHL. I thank you very much and I thank you, Mr. Chairman.

Senator GREGG. Thank you, Senator.

Senator Cochran was not able to join us today, but has submitted a statement for the record.

[The statement follows:]

PREPARED STATEMENT OF SENATOR THAD COCHRAN

Mr. Chairman, thank you for accepting the job of chairing this important Subcommittee. You have some big shoes to fill, but I know you can do it.

Mr. Secretary, you are off to a great start. We appreciate your visit to my State and the way you have moved quickly to identify the challenges facing the Department of Homeland Security.

We need strong leadership in this important job and I know you are well-qualified to provide it. The main challenge is to coordinate the Nation's resources in this effort. Our greatest strength is the ingenuity of our public servants and citizens. With the proper leadership, we will meet these challenges.

Our role on this Subcommittee is to provide you and your Department with the resources needed to carry out your responsibilities and we will work with you to identify the priorities.

TSA

Senator GREGG. Let me pick up on your question, because the TSA is an issue that I think just every American is a little frustrated with sometimes. And I guess my question is this, and it is a philosophical one.

Once we hardened the doors and took away the capacity to use airplanes as missiles, private passenger airplanes as missiles, we changed the dynamic of the threat fundamentally. And yet we have created an agency which has what, 45,000 people? And here we are on a border where we have 10,000 agents, and we probably need 20,000 agents to do it right, have to be well trained, obviously, and there has to be an infrastructure to support them, and all that.

Are we basically reacting to yesterday's threat? We have port security issues. We have border crossing issues. And yet we put a huge amount of resources into airport security without, it appears, any significant improvement in security relative to the ability to get weapons through security, and having addressed the fundamental threat, which is an airplane used as a missile.

Secretary CHERTOFF. I asked myself that question coming into this job as well, and if I can just take a minute to break it into several different issues.

AVIATION SECURITY

First of all, there is the issue of aviation security in itself. Are we optimally focused on what the real threat is? And I think you have put your finger on it, Mr. Chairman, when you indicated the first thing we have to be really pretty tough about is recognizing that there are degrees of consequence that we are worried about.

The aircraft as a missile is the worst consequence. It is bad to have an aircraft blown up in midair, too, that may be a somewhat less significant consequence. It would certainly have tremendous ramifications across the airline system, and then there are yet other possible actions. So we have to frame the issue that way.

We do have hardening of cockpit doors. There are other steps we can and should take to prevent the aircraft used as a missile. That might very well counsel to change or moderate or adjust our current levels for screening with respect to certain types of items, and increase our screening for other types of items.

Maybe to use the proverbial example of nail clippers, which I do not think are being screened for now anyway, but maybe we need to be a little less worried about metal cutlery and a little more worried about explosives. So that is within the issue of aviation, and that is something we are actively looking at now.

EMERGING ISSUES

The second issue is making sure our attention is not distracted away from emerging issues. We are looking heavily at the issue of rail security. We are looking at the issue of cargo. We have deployed non-intrusive inspection technologies. Those are very good. I have seen them work myself. You may very well have it as well. That is a positive step we are paying attention to.

And as I said to Senator Murray, we are looking at this whole issue of cargo movement to see how we can use the modern supply

chain, techniques, and technology to really make sure we are doing what we need to do to protect against bad cargo. So I am completely on board with the idea of making sure we are not distracted by the thing we have already done, spending a lot of time on that because we know how to do it and it is comfortable, rather than looking at the stuff we have not done as well that we need to elevate up.

MOVEMENT OF RESOURCES

Senator GREGG. Yes. I agree. And I am glad you are looking at it that way. But I am asking, are we taking it to the next step, which is, you know, we are spending, I think, I have forgotten the numbers, $3.5 billion, some outrageous number, on TSA. But should we be moving that number to border patrol? Should we be taking a large percentage of that employee base and moving them over, if not as a direct personnel shift, as at least a resource shift, reducing the number of personnel at TSA and moving people to border patrol where we know we have a bigger risk right now relative to the potential threat.

Secretary CHERTOFF. Well, I do not know, Senator, that I would do that, because I do not know that I would say that there is a bigger risk. I mean I do not want to go to the other end and minimize the aviation risk too much. I mean the reality is, even putting aside the aircraft as a weapon, if we were to have a series of explosions on airlines, or something comparable, that would have a humongous effect on the national economy and a humongous effect on our ability to move around.

We want to have a smarter deployment of resources in the aviation security area, but we want to have the outcome be very, very good security in terms of things we are worried about. I do not know that, for a whole host of reasons, including training and skill sets, that we could simply move TSA people into——

Senator GREGG. I do not think you could——

Secretary CHERTOFF. Yes.

Senator GREGG [continuing]. Move people, but I am talking about the dollars to support those people. I mean the threat to the aircraft now is, as you mentioned, an explosive probably more than a weapon, because you cannot take control of an aircraft with a weapon, theoretically. I mean maybe it is possible if you have a big enough weapon on board. But if an explosive is the threat, is it not really a technology response to that rather than a people response?

Secretary CHERTOFF. I think that is right. I think ultimately the way to move to the level we need to get is technology, because I think there is an inherent limitation. People are limited by the technology. I mean you can be the best trained and the most well-intentioned person in the world. If your detection device does not let you get sufficient granularity or make distinctions between types of things, between the dangerous and not dangerous, that is limitation. So we need to get the technology to where it needs to do.

That might ultimately allow us to reduce workforce, although I do not want to make a prediction that it is going to happen in the short term, because I still think there is an element of human judgment that you bring to bear that is still very important. But there

is no question that we have to both invest in the technology, but also, as I said, roll out the technology we have and start to use it, rather than continuing to fuss around, you know, everybody having—I do not want to minimize privacy concerns. I have them as well. But we need to come to grips with them, we need to adjust for them, we need to reach a decision about how to accommodate them, and then we need to start to move forward.

THEFTS OF LUGGAGE OF PASSENGERS

Senator GREGG. The problem I see coming here—well, this is just one element of the issue, but relative to TSA—is that with a report of literally thousands of thefts occurring in luggage of travelers, and it appears that a high percentage of those thefts are the responsibility or the actions of Federal employees of TSA, that we are probably going to have to institute a major camera program or something to monitor the search of luggage by employees. And so we are going to end up spending significant resources to protect ourselves from the employees who are supposed to be protecting us from damage on the planes. As a taxpayer I find that uniquely frustrating. And as a policymaker, I find it to be a terrible waste of resources.

Secretary CHERTOFF. I agree. I mean, obviously, pilferage is completely unacceptable. And it is a bad State of affairs if we have to spend money protecting ourselves from people who are protecting us.

I am convinced, of course, the majority of screeners are terrific and ethical and——

Senator GREGG. I am sure that is true.

Secretary CHERTOFF [continuing]. Things like that. But you are right.

Senator GREGG. The track record, unfortunately, is that there is a large amount of—there is a big problem here.

Secretary CHERTOFF. And that is why—I agree with you. The technology is really the way forward in terms of getting ourselves to where we need to go.

DHS INTELLIGENCE ROLE

Senator GREGG. In the area of intelligence, I am not sure I understand, and I am new to this. Since the issue was moved out of CJS, and I am new to this committee, I am not sure I understand what the Department sees as its role in intelligence right now. It is clear that there was a conscious decision to give up the actual collection and analytical effort to other Federal agencies. You got IAIP, which I guess is stood up, but it seems to continually to be raided for its revenues.

What do you see as the intelligence function of Homeland Security, of the Agency, in relationship to these other agencies and internally?

Secretary CHERTOFF. Well, first of all, I think we are definitely in the business of collection. Let me explain what I mean by collection. We have thousands of interactions every day at the border and investigations with ICE agents at the airport. And many of those yield information which I would consider to be of intelligence value.

We are in the process now of increasing our use of that intelligence and our collection of that intelligence, doing a number of different things. For the first time, we are putting reports officers into the operational units, meaning people who will look at the operational flow of information and say, wait a second, this is not just a trivial interaction. This is a piece of information that is useful from an intelligence standpoint. Let us make sure we capture it and send it up to our information analysis section so it can be fused and collected and then ultimately transmitted to the community.

We have started to do that. I have seen the results. The Federal Air Marshals actually use modern technology to in real-time report things they see on airplanes that could have intelligence value in terms of suspicious behavior, so we get identification of people that we need to be on the lookout for and we can then put that into a system that all of law enforcement can have access to. So we have a tremendous potential to be collectors, which I want to make sure we are fully exercising.

The second piece of that is, once we get ourselves to where we need to be in collection and we continue this process, we can contribute to the whole community by putting that into the NCTC, which is the counter-terrorism center. And that was set up by Congress in the Intel Reform bill as the kind of fusion point for counter-terrorism intelligence.

By putting that information in there, we are sharing with the community. We are also contributing. And my experience is that when you contribute as a partner, you then get full partnership. So I view that as a very critical piece of what we need to do to make sure we are sitting at the table with respect to everything else that comes in from the other parts of the intel community—overseas stuff, signals intelligence, human intelligence in other countries.

The third piece is, as partners at the table, we need to be able to look at all that stuff and operationalize it. And right now in the Department we are talking about how we want to enhance the ability of IA, of information analysis, to collect all this from the central pool that we have at the NCTC, to translate into operational mandates to make sure we make adjustments at the border and other adjustments so that we actually make use of this intelligence.

So that is my vision of where we are going. I have met with the acting head of NCTC. I have met with other main players in the community, and I have expressed my very strong personal interest in seeing that we get this done.

USE OF IDENT, IAFIS AND US VISIT

Senator GREGG. Where do you see the technology situation relative to IDENT, IAFIS, and also relevant to US VISIT.

Secretary CHERTOFF. As you know, Senator, IDENT was, I guess, the system that was stood up under the old INS, pre-9/11. IAFIS is a system the FBI set up. Right now, as I understand it, we have the ability at ports of entry, at Customs and border-patrolled posts, to access both of those databases at the same time. They are separate databases, but we can run prints against both of those databases.

Now IAFIS is a ten-print database. So ultimately there is a decision which we need to reach about implementing a way to get to making effective use of a ten-print database. And I think there is a technological challenge there and there are some policy decisions that we are in the process of making.

I think we made a lot of progress in making both databases accessible at a single point at the border and at our border and customs stations. We have not fully exploited the technology. We need to continue the process of building an architecture that lets us get the maximum use out of our biometric data that we capture and run it against the maximum number of databases.

Senator GREGG. US VISIT.

Secretary CHERTOFF. We have deployed it at our airports. We have deployed it at seaports. We have deployed it at our 50 most significant land border entry points. We are starting to pilot it at the exit points.

It has been very successful. I have seen it operate. It is fast. We have captured people on it that we should not be letting in the country and we have been able to turn them away.

You know, it can be improved, and we can make better use of it. But it is, I think, the key to the next generation of keeping our borders secure.

PREPARATION FOR BIOLOGICAL ATTACK

Senator GREGG. What do you see your success relative to preparation for an attack that might be biological?

Secretary CHERTOFF. As you know, Mr. Chairman, we just finished TOPOFF III, which was a massive exercise done internationally and in two States, which had a hypothetical biological attack. I have met with Secretary Levitt. We have talked about some preliminary lessons learned. We are doing a very comprehensive review of that to make sure that we have the following things in place.

First of all, we have an adequate stockpile of the kinds of antidote where we have them or vaccinations where we can have them against the likely agents; that we have very particular plans in place for distributing that type of vaccine or that type of antidote, if we should have an attack; and that we are fully integrated across the board in terms of our standards for reporting biological incidents.

You know, we had that anthrax false scare about a month ago. We did a very vigorous review of that. We have made some changes now with the Defense Department as well as with our Department in making sure we are operating with the same set of standards. And we are now working across the Federal Government to test to make sure everybody has got the same template for what we are sensing, what constitutes a positive finding, when do we get to the point that we need to take steps to get people inoculation or antidote.

Again, we have got progress to make. I think we have learned a lot of lessons, both recently and going back, and I think we have a program in place to start to move ourselves to a position of readiness for what, I agree with you, is one of the two or three worst-case scenarios that we have to be prepared for.

TOPOFF EXERCISE

Senator GREGG. It is interesting. When I was on the Commerce and Justice Committee, when I was chairman of that, we began the TOPOFF exercise program over the strong resistance, ironically, of almost every Federal agency. We simply insisted we do it. It has now turned into a very successful program.

But I was interested when I was at the TOPOFF exercise this year that neither New York City nor Los Angeles were—I guess Washington, marginally, participated in the major TOPOFF exercises there. I guess that is because they have not been asked to do it, or agreed to do it.

It would seem since they are priority areas, that we would want in our TOPOFF exercises to go to places where the actions may actually most likely occur.

Secretary CHERTOFF. I was not involved in, I guess, the selection for 2003 and I guess the selection for the next one was made before I came on. I know people do apply and then a decision is made.

I know Chicago did the last one, I think, TOPOFF II. Northern New Jersey and Connecticut are part of the New York metropolitan area, so we did exercise some pieces of this.

I agree, at the end of the day—by the way, we should be doing tabletop exercises, meaning not maybe the full TOPOFF, but something all across the board. I wondered myself how valuable it was, and I have to say I was convinced that it was of tremendous value.

I learned a lot and I think a lot of people learned a lot by testing the system. So I am in favor of doing at least some kind of exercise as an important part of our preparedness.

Senator GREGG. Well, I would hope that the Department would take a look at whether or not we should not do them to some degree based on the threat criteria versus just the willingness of a governor to participate or a State to participate.

Well, I appreciate your time. I have two last questions.

STABILIZATION OF SENIOR MANAGEMENT

There is a large amount of open slots and acting slots. What do you see relative to senior management getting it up and stable?

Secretary CHERTOFF. I am concerned, obviously, as a secretary who does not want to have to do every job himself, to make sure we have very good people. I am pleased to say we have filled some of those spots. We have got others where we have nominations pending before the Senate. Obviously, the more quickly we can fill those spots the better.

We want to get the right people. We want to get people who have the energy and the creativity to make the Department what I think it can be, going to the next level. And part of what we are trying to do, frankly, is to recruit and bring people in to top slots that bring a variety of different perspectives.

I think it is good to have people with military backgrounds, people with law enforcement backgrounds, people with business backgrounds, people with first responder backgrounds, because ultimately our success involves merging functions, and that means merging skills.

So we are actively out there finding the right people. The President has got some nominations in and has made some appointments already. And I am, for personal as well as professional reasons, very eager to get this process done as quickly as possible.

NEED FOR ADDITIONAL ASSISTANCE FROM THE SUBCOMMITTEE

Senator GREGG. And lastly, beyond approving your budget, which I suspect we will do and actually probably do more than your request, is there anything this committee can do to be helpful in the legislative or other areas?

Secretary CHERTOFF. There may well be as we complete this process of second-stage review that we will have some recommendations to make for some legislative action that would align us better in terms of what we need to be able to generate for outcomes. And I will look forward to when we get to a point that we can, I think, have some recommendations sitting down with you and the other members of the subcommittee and talking about those, and trying to adjust as much as possible.

One thing I do want to thank you for is the subcommittee's commitment to make sure that we get real discretion in terms of using risk management as a way of handling issues like funding and all of our functions, as opposed to—I know from what I read in the paper that the lobbyists continue to view DHS as a wonderful—I think one used in a newspaper article the term "pots of money" for the clients.

I do not view us as pots of money. I view us as having an obligation, both as stewards of the public money and as stewards of the public safety to make sure that what we do with our money that Congress appropriates for us is based on sound judgment and risk management, not based on lobbyists trying to get their clients into the pots of money.

Senator GREGG. Well, I agree with you. In this issue, first off, funds should be distributed on the basis of threat; and, secondly, earmarks should be used only in the extreme situation where Congress has a very legitimate policy reason that feels that the Administration is not pursuing. So I presume that will continue to be this committee's approach.

Secretary CHERTOFF. Right. Thank you very much, Mr. Chairman.

Senator GREGG. Thank you, Mr. Secretary, for all your time. I appreciate your courtesy.

Secretary CHERTOFF. Thank you.

ADDITIONAL COMMITTEE QUESTIONS

Senator GREGG. There may be members who wish to submit questions to the Department. As is typical, we presume they will be answered in a prompt way.

Secretary CHERTOFF. Absolutely.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED BY SENATOR JUDD GREGG

COMPREHENSIVE REVIEW OF THE DEPARTMENT

Question. Secretary Chertoff, in your first speech after being confirmed Secretary of Homeland Security; you announced that you had initiated a 60 to 90 day comprehensive review of the organization, operations and policies of the Department as a whole. You discuss that review more fully in the prepared statement which you have submitted to the Committee.

You are now some 30 days into that review. Can you share any of your preliminary findings with us at this point, including any preliminary conclusions you may reach on what's working and what is not?

Answer. The comprehensive review of the Department is complete. I gave a speech on this topic on July 13 where I outlined our preliminary conclusions, the text of which can be found at the following website: http://www.dhs.gov/dhspublic/display?content=4597.

Question. You indicate that the Deputy Secretary Michael Jackson is overseeing this review and has selected a team of Department officials to look at cross-cutting issues and determine how departmental resources and programs can be effectively used to achieve our security goals. Do you intend to involve others outside of the Department in this review?

Answer. Other Federal agencies were included in this effort where appropriate. Moreover, while the committee was comprised exclusively of DHS employees, we considered recommendations from our state, local, tribal, and private sector partners, among others.

Question. What cross-cutting issues are you looking at? How were those determined?

Answer. We looked at all areas to examine the mission and work of all DHS elements to ensure that we have the best organization, operations, and policies possible to most effectively protect and safeguard this Nation. Notable examples of areas in need of greater cross-cutting included maritime cargo security, information sharing, and immigration policy. As a matter of process, the senior leadership of the Department was asked to identify the key issues that should be evaluated as part of the comprehensive review. The issues were then reviewed by me and the Deputy Secretary to identify further and refine cross-cutting topics that encompassed the key issues identified by the senior leadership.

Question. As you are aware, we are fast-approaching the time when the Committee will make decisions on the Department's appropriations for fiscal year 2006. The budget request now before us is based on the Department's current structure and operations. Therefore, we are very interested in staying abreast of what changes are being contemplated and recommended.

What is your time frame for concluding the review and for making any changes you determine are necessary, including those that might be done through your reorganization authority or require the submission of a legislative proposal or fiscal year 2006 budget amendment to the Congress for consideration?

Answer. The comprehensive review of the Department is complete. I gave a speech on this topic on July 13 where I outlined our preliminary conclusions, the text of which can be found at the following website: http://www.dhs.gov/dhspublic/display?content=4597.

We have also outlined our reorganization plan in detail in our Homeland Security Act Section 872 report, which was submitted to Congress after we completed the Second Stage Review (2SR). Further, a few of our recommendations will require congressional action. We have submitted legislation accompanying the 2SR Report that, once passed, will effectuate the reorganization changes we believe are necessary for the Department's success. It is important that our draft legislation be passed in its current form.

INTERNATIONAL PARTNERSHIPS

Question. How will the Security and Prosperity Partnership of North America announced last month promote and foster a mutually beneficial, common security system along our borders?

Answer. On June 27, in Ottawa, Canada, U.S. Department of Homeland Security (DHS) Secretary Michael Chertoff and Department of Commerce Secretary Carlos Gutierrez and their government counterparts in Mexico and Canada released the first report of the Security and Prosperity Partnership (SPP) of North America that identifies initial results, key themes and initiatives, and work plans that further promote the security and prosperity of North America. The SPP countries agreed to these, and other, North American security goals:

—*North American Trusted Traveler Program.*—All three countries have agreed to create a single, integrated program for North American trusted travelers by 2008. Individuals applying for trusted traveler status would be able to apply for the program and pay relevant fees in one transaction. Enrolled participants would have access to all established trusted travel lanes at land crossings, airports and marine programs. A single North American Trusted Traveler Program embodies the intent of the SPP to establish optimum security goals while accelerating legitimate cross-border trade and travel. The United States will also be working cooperatively to identify Western Hemisphere travel document standards required under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).

—*Preparedness and Incident Management Systems Integration.*—The United States, Canada and Mexico have agreed to transform North American preparedness for response to large-scale incidents by establishing protocols for incident management that impact border operations within 12 months. Protocols will also address maritime incidents, cross-border public health emergencies and cross-border law enforcement response. The SPP countries have also committed to ensure interoperable communications systems and to participate in preparedness exercises that will strenuously test these protocols. In addition, the three countries will participate in a preparedness exercise in anticipation of the 2010 Vancouver/Whistler Winter Olympics.

—*Border Enforcement.*—The United States and Mexico will form joint intelligence-sharing task forces along the U.S.-Mexico border to target criminal gang and trafficking organizations and reduce violence along the border. The United States and Canada will coordinate maritime enforcement programs to address the huge volume of boat traffic in our shared waterways.

—*Facilitated Flow of Legitimate Cargo and Travel Across Land Borders.*—The United States, Canada and Mexico have agreed to review our transportation and border facility needs, in partnership with stakeholders, and develop a plan to prioritize future port-of-entry-related infrastructure investments. All three countries are considering programs to reduce transit times and border congestion by expanding trusted traveler programs to additional ports of entry and partnering with public and private sector stakeholders to establish "low-risk" ports of entry for the exclusive use of those enrolled in our trusted trade and traveler programs. The United States and Canada, along with local stakeholders, are working to reduce the transit times by 25 percent at the Detroit-Windsor gateway within 6 months, and all three countries are exploring ways to expand this innovative 25 Percent Challenge to other North American land border crossings within the next 18 months. By December of this year, the United States and Canada governments expect to complete an agreement on a pre-clearance pilot program at the Peace Bridge in Buffalo, NY, contingent on Canadian legislative amendments. Within 6 months, both countries will also develop a plan to expand the Vancouver NEXUS-Air pilot program to other United States air pre-clearance sites in Canada and examine the feasibility of expanding the eligibility for NEXUS-Air to include Mexican nationals.

—*Shared Watchlists and Integrated Traveler Screening Procedures.*—The United States, Canada and Mexico have agreed to strengthen information sharing related to terrorists and criminals. Effective information exchange among North American countries is essential to strengthening our capability to prevent acts of terror within and outside North America. The United States, Canada and Mexico have also agreed to establish compatible screening standards for land, sea and air travel to identify and prevent high risk travelers and cargo before they depart for North America. Additionally, recommendations will be made on the enhanced use of biometrics in screening travelers destined to North America. On an ongoing basis, the SPP will enable all three countries to address and resolve gaps in cross-border information sharing. Ultimately, all travelers arriving in North America will experience a comparable level of screening.

—*Maritime and Aviation Security.*—The SPP countries will also be working toward comparable standards for hold baggage and passenger screening, implementing no-fly programs throughout North America, and developing new protocols for air cargo inspection. Likewise, we will also be working to develop compatible maritime regulatory regimes and to strengthen information sharing and coordinated operations in the maritime domain.

Question. What role will the Department have in this initiative?

Answer. The Department is taking a lead role in implementing the SPP's Security Agenda, in cooperation with other Federal agencies. The Department has been tasked with convening working groups with Canada and Mexico to develop and implement concrete work plans and specific timetables to meet the broader goals asso-

ciated with the SPP's Security Agenda. Additionally, the Department is continuing to work with the Department of Commerce, which is taking a lead role in the development and negotiation of a complementary Prosperity Agenda, and the State Department, who is taking a coordinating role to best align efforts.

Question. Under the Western Hemisphere Travel Initiative recently proposed, how will the Department ensure that NEXUS is universally available on the Northern Border by the time the new document requirements are imposed at land ports of entry?

Answer. To keep pace with the potential impact of the WHTI, DHS plans to expand the enrollment process as well as potentially opening additional ports of entry with regards to NEXUS program along the Northern Border. Concurrently, we are also examining potential resource needs to accommodate additional demands of these programs as a result of the WHTI. As part of the Western Hemisphere Travel Initiative (WHTI), DHS will be issuing an Advance Notice of Proposed Rulemaking (ANPRM) to solicit comments from the public and affected entities regarding the requirements and alternative documents that may be designated by the Secretary to demonstrate citizenship and identity for entry. As required by the President, we are and will continue to examine, in response to comments on the ANPRM, other potential documents that may be designated for the land border environment in advance of the January 1, 2008, deadline.

Question. How is the Western Hemisphere Travel Initiative going to work with US VISIT, since US VISIT is implementing the tracking of entries and exits across our borders?

Answer. The Department will coordinate the implementation of the Western Hemisphere Travel Initiative with US VISIT enrollment to facilitate travel and to ensure security at our Nation's borders.

Question. Will US VISIT manage this initiative?

Answer. US VISIT is playing an active role in this initiative.

MANAGEMENT AND STAFFING

Question. Executive agencies need to rely on a stable bureaucracy to keep things running during leadership transitions. The Department has significant vacancies in top leadership positions and significant turnover in senior- and mid-level managers.

Mr. Secretary, what is your time frame for putting your management team together?

Answer. I agree that we do not want any unnecessary delays in filling these vacancies. At the same time, however, we want to make sure we get the right people to fill these positions. We want to bring people on board who have the energy, creativity, and a variety of perspectives to further the Department's mission and enable us to move to a next level of achievement. The President has forwarded several nominations to the Senate for consideration, and we will move as quickly as possible to fill remaining vacancies.

Question. What disruptions are the current vacancies in confirmed leadership positions having on the Department?

Answer. For every vacancy in a leadership position, an employee has been identified to serve in an Acting capacity until a person is confirmed to fill the position. While we are striving to fill vacancies as quickly as possible, these dedicated employees have risen to the challenge of fulfilling the requirements and obligations of these leadership positions and have maintained the Department's activities and efforts.

Question. What is your assessment of the difficulties the Department has experienced attracting, hiring or keeping qualified personnel and what is being done to correct this situation?

Answer. DHS faces many of the same problems with recruitment and retention that plague most Federal agencies—cumbersome recruitment and hiring processes, lack of competitive salaries, and poor performance management and recognition programs. Fortunately, our mission is inspiring to many, and we usually are able to attract well-qualified candidates in spite of these impediments. However, we need to continue to improve to stay competitive for the very best candidates.

DHS has a Human Capital Strategic Plan that aggressively addresses effective recruitment, development, compensation, succession management, and leadership issues. A major priority in this Plan has been streamlining the DHS hiring processes to meet the Federal standard of 45 days. A common DHS recruitment brand with state-of-the-art recruitment materials has been established to ensure effective and consistent external representation of DHS in the hiring process. These initiatives will enable DHS to maintain viable recruitment networks, particularly in mission critical occupations.

A consolidated DHS Workforce Plan was completed in March 2005 that establishes a baseline for workforce trend analysis for mission critical occupations. This Plan also enables component organizations to plan well in advance for upcoming recruitment needs. Where potential occupational gaps exist, human capital strategies will be identified and implemented.

MAX, the new human resource system for DHS, will have both market-sensitive pay and a robust performance management process, which will enable DHS to be more competitive in its recruitment process and more effective in retaining and motivating employees.

DEPARTMENTAL REORGANIZATION

Question. Reorganizing seems to be a sport within the Department these days. At what point does continued reorganization impede the ability of the Department to get its job done?

Answer. The Department's reorganization plan will significantly enhance, not impede, our ability to meet our current and future objectives. The Department recently passed its 2 year anniversary mark. In that short time, 22 separate agencies were brought together, and the work of integrating those agencies into a working structure began. We are now taking advantage of 2 years of experience, an opportunity unavailable to our predecessors, to implement a reorganization plan that takes the Department to the next level, best positions us to manage our current and future responsibilities, and helps us better adapt to current and future threats and disasters.

Question. On the other side of this issue is the continued viability of the current organization of the border management agencies. DHS has moved organizations into ICE; it has moved organizations out of ICE. We have poured almost $800 million in additional resources into ICE over the last 2 years, including $276 million in the Senate-reported fiscal year 2005 emergency supplemental. Is ICE a viable stand-alone organization or should it be broken up and have its responsibilities merged into other parts of the Department of Homeland of Security such as CBP?

Answer. As you know, the Department looked at a variety of organizational issues as part of the second-stage review process, which helped clarify where the Department needs to be organizationally to ensure effective implementation of our critical missions. We considered whether ICE should remain a stand-alone entity, and decided that it should. We believe it's in the Department's best near and long-term interest that ICE not be merged with another component, CBP in particular. To reach this decision, we focused on the operational mission needs of both CBP and ICE, not on the near-term management challenges. I take seriously the challenges the Department has faced concerning ICE and appreciate the difficult but necessary choices Congress has made in providing new funding to address its needs. I am confident, however, that ICE has made substantial improvements in financial management this year. Not only have substantial new resources been provided, but a new management team is taking shape.

HOMELAND SECURE DATA NETWORK

Question. The fiscal year 2006 President's budget contains the first request to the Appropriations Committees regarding the Homeland Secure Data Network (HSDN). Why should funds be appropriated for HSDN now when the Department has seen fit to absorb $79 million in the past 2 years and not seek proper appropriated dollars for this purpose?

Answer. Anticipating the need to share intelligence and other information securely to fulfill its homeland security mission and to ensure efficient and effective use of scarce funds, the DHS CIO streamlined and merged disparate classified SECRET network initiatives within the Department into a single secure network called the Homeland Secure Data Network (HSDN). Existing agency funds for these initiatives were used to stand up this critical infrastructure. However, the fiscal year 2006 funding request is needed to use the additional funds to expand HSDN into a major, secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations in the common goal of protecting our Nation and its citizens. An expanded HSDN will provide Secret connectivity and the required efficient information sharing capability to the non-DOD government community.

Question. Does DHS have the ability to share classified information today? If yes, why does a stand-alone system need to be built for DHS?

Answer. Today only a few Homeland Security components have the ability to share classified information over the DOD's SIPRNet. The present HSDN capabilities currently support over 30 DHS sites and will expand classified connectivity to

60 DHS sites in the next 2 months. DHS, and the non-DOD, government sector (including other Federal, State, local and tribal government) require the infrastructure and the processes and procedures to share classified information wholly effectively. The HSDN is an essential step that will allow the efficient sharing of classified information required for the mission of protecting the homeland. DOD policy in the wake of September 11, 2001, has been to migrate non-Defense, homeland security classified communications off SIPRNet and onto the HSDN. The DOD policy is based on the desire to ensure the SIPRNet can effectively support the war-fighting mission. DOD and DHS have established a joint, controlled interface between SIPRNet and DHS to provide for several levels on connection between HSDN and SIPRNet based on policy.

Question. Why isn't the budget for this project consolidated? Why is it being funded by specific organizations of the Department?

Answer. HSDN has rapidly evolved from an initially conceived agency specific network to a presently deploying DHS-wide network based on mission needs. HSDN is funded by charging each agency based upon the HSDN usage by that agency during a yearly time period. The working capital fund has served as a method to consolidate organizational element funding to support a single HSDN capability. The specific organization funding level will be adjusted as the usage requirements of each agency change over time.

Question. What is the rationale for how much each agency is being charged for HSDN?

Answer. The HSDN rationale for charging each agency is based upon the HSDN usage by each agency during a yearly time period. Presently, a formula has been developed that charges an agency based on its HSDN participation. Basically, this formula develops a percentage by agency based on the number of locations (sites) and the number of terminals (workstations) installed. The number of sites (large, medium and small) and seats is a usage-based cost model. Site size is an industry standard such applied by an internet service provider who charges are based on the size of your site (bandwidth of the connection). The usage is also determined by the number of seats. While some sites will allow multiple users for a single workstation, the number of seats sets the usage level at the site.

Question. The Information Analysis and Infrastructure Protection Directorate has in its budget the Information Sharing and Collaboration program. One of its responsibilities is "fostering collaboration among various levels of government and the private sector through the creation of a secure information sharing environment capitalizing on existing opportunities". How does this project relate to HSDN? Are these duplicative or complementary efforts?

Answer. These are complementary efforts. In May 2004, my predecessor, Secretary Ridge, created the Information Sharing and Collaboration (ISC) initiative to coordinate and facilitate efforts throughout the Department and with our customers and partners, particularly the Federal, State, tribal and local governments, and the private and international sectors, to affect change and improve information sharing and collaboration to secure the homeland. Since then, the importance of information sharing has been made more evident through the publication of numerous reports (such as the 9/11 Commission Report, the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, and GAO studies), the issuance of new Executive Orders (for example, E.O. 13356), and a new public law, Public Law 108–458, the Intelligence Reform and Terrorism Prevention Act of 2004. Section 1016 calls for the creation of an Information Sharing Environment, which will require the sharing of information at levels including unclassified, sensitive but unclassified, SECRET, and perhaps higher.

Anticipating this need to share intelligence and other information securely to fulfill its homeland security mission, DHS is streamlining and merging disparate classified SECRET networks into a single, integrated network called HSDN. We envision that HSDN will become a major, secure information thoroughfare joining together intelligence agencies, law enforcement, disaster management, and front-line disaster response organizations in the common goal of protecting our Nation and its citizens. The ISC does not build systems or operate networks, such as the HSDN. The ISC initiative ensures system and network investments support DHS' information sharing mission.

OFFICE OF SCREENING COORDINATION AND OPERATIONS

Question. The President's budget proposes to create the Office of Screening Coordination and Operations, or SCO, within the Border and Transportation Security Directorate. How do you see this new office contributing to the Department's ability

to implement the 9/11 Commission recommendation regarding a comprehensive screening system with system-wide goals?

Answer. I support the concept of a Screening Coordination and Operations (SCO) Office, and developed plans through the 2SR process to meet the goals of the office. Consistent with the 9/11 Commission recommendations, HSPD–11 and HSPD–12, the SCO office will develop a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers and leverage current investments in screening systems and tools. The SCO will harmonize IT architecture, uniform redress policies, and provide coordinated or shared services such as card production, biometric/biographic databases, as well as set DHS standards for information technology enterprise architecture and global enrollment systems/processes. The SCO office will develop a consistent approach for outreach in the areas of privacy, civil rights, and will coordinate R&D efforts. DHS will set up the SCO office in fiscal year 2006, as reflected in the Department's revised fiscal year 2006 request.

Question. Should the SCO have actual operational authority for various screening programs as proposed, or should it focus on the integration and coordination function, for example the development of the Department-wide credentialing standards necessary across so many programs involved in this activity?

Answer. I support the concept of a SCO Office, and developed plans, through the 2SR process, to meet the goals of the office. Consistent with the 9/11 Commission recommendations, HSPD–11 and HSPD–12, the SCO office will develop a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers, while leveraging investments in screening systems and tools. The SCO will harmonize IT architecture, establish uniform redress procedures, and provide coordinated or shared services such as card production, biometric/biographic databases, common DHS standards for information technology architecture, and global enrollment systems/processes. The SCO office will develop a consistent approach for outreach in the areas of privacy, civil rights, and helping to ensure coordinated R&D efforts. DHS plans to set up the SCO office in fiscal year 2006.

Question. At the same time that significant programs are being proposed to be moved from Customs and Border Protection and the Transportation Security Administration, the President's budget does not propose moving the operational responsibility for any of the programs that incorporate screening of applicants out of U.S. Citizenship and Immigration Services (CIS). In order to ensure that there is the closest possible coordination across screening programs, should CIS screening programs also be moved to the SCO? Why wasn't CIS included?

Answer. I support the concept of a SCO Office, and developed plans through the 2SR process to meet the goals of the office. Consistent with the 9/11 Commission recommendations, HSPD–11 and HSPD–12, the SCO office will develop a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers and leverage current investments in screening systems and tools. The SCO will harmonize IT architecture, uniform redress policies, and provide coordinated or shared services such as card production, biometric/biographic databases, as well as set DHS standards for information technology enterprise architecture and global enrollment systems/processes. The SCO office will develop a consistent approach for outreach in the areas of privacy, civil rights, and will coordinate R&D efforts. DHS will set up the SCO office in fiscal year 2006, as reflected in the Department's revised fiscal year 2006 request.

US VISIT

Question. How do you plan on addressing the issue of integration of the two fingerprint systems—IDENT at the Department of Homeland Security and IAFIS at the Federal Bureau of Investigation?

Answer. The US VISIT Program, working closely with CBP and ICE, and the Departments of Justice and State, leads the IDENT/IAFIS integration efforts. DHS' systems receive daily updates from the FBI with information from a variety of criminal and threat-related databases. There are several different ongoing efforts to bring about interoperability between the IDENT and IAFIS.

—DHS (US VISIT) established an integrated project team (IPT) with the FBI (Criminal Justice Information Services or CJIS) to address the policy, business requirements, and technical aspects of integrating IDENT and IAFIS. This IPT has made significant progress in resolving many of the long-standing issues in the DOJ Office of the Inspector General's report. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

—Integrated IDENT/IAFIS workstations will be deployed to sites that will have US VISIT—115 airports, 15 seaports, and 165 land border ports of entry—as well as to specific ICE field office locations, by the end of calendar year 2005.

—DHS and DOJ have completed a Memorandum of Understanding (MOU) to resolve data access and privacy issues concerning FBI usage of US VISIT data.

Question. Are there any DHS/FBI jurisdiction issues hampering the integration effort?

Answer. DHS and DOJ/FBI have achieved an effective working relationship on integration. As noted above, DHS (US VISIT) and FBI (Criminal Justice Information Services or CJIS) have established an integrated project team (IPT) to address the policy, business requirements, and technical aspects of integrating IDENT and IAFIS. This IPT has made significant progress in resolving many of the long-standing issues originally referenced by the DOJ Office of the Inspector General. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

GLOBAL SUPPLY CHAIN SECURITY

Question. Mr. Secretary, in your written testimony you used cargo container security as an example of an area where the Department could do a better job coordinating across all departmental efforts. What impact have the various programs the Department is running had on cargo container security so far? What can be done better?

Answer. Since September 11, 2001, the various cargo security programs now operated by the Department have made great strides in moving us towards a system of security that prevents the use of the supply chain in a terrorist attack while enhancing supply chain efficiency and reliability. Before September 11, most cargo security efforts were centered at the port and based on local perceptions of risk. Today we have improved data reporting through the 24 Hour Rule supported by centralized targeting at National Targeting Center. This capability coupled with the Container Security Initiative has allowed us to revolutionize the customs function by allowing us to interdict threats before they leave for the United States.

Our current programs and capabilities have laid the foundation for a truly 21st century international trade system, one that will support growth in international trade and our security interests. Other efforts, such as Operation Safe Commerce, the Advanced Container Security Device program and the Advance Trade Data Initiative, will provide us with the knowledge and tools to help us get there. To that end, I am reviewing the status of DHS's cargo security efforts, how they can be further strengthened and how we can further transform the system to ensure the United States security and economic needs are met.

Question. What is the status of the final report on Operation Safe Commerce, and when will it be submitted to this Committee?

Answer. The report on Operation Safe Commerce (OSC) requires submission of program information from OSC's three participating load centers. One participant's input was behind schedule but has recently been received. This information will be integrated into a report and distributed for review by relevant experts. We expect the report to be issued by the end of December 2005.

Question. What more should be done in this area?

Answer. I am reviewing the status of DHS's cargo security efforts, how they can be further strengthened and how we can further transform the system to ensure the United States security and economic needs are met.

AGRICULTURAL INSPECTIONS

Question. The April 14, 2005, U.S. Department of Agriculture, Office of Inspector General Report regarding coordination between the Department of Homeland Security and the Department of Agriculture indicates that coordination has been less than adequate for the last 2 years. Specifically, the report mentions APHIS personnel being denied entry to ports-of-entry to conduct its required regulatory reviews. What are you doing to change this situation?

Answer. CBP and the U.S. Department of Agriculture (USDA) Animal and Plant Health Inspection Service (APHIS) signed in February 2005 Appendix 8 to Article 8 of the Memorandum of Agreement (MOA) between DHS and the USDA. The MOA establishes and enhances coordinated actions and operations between the two agencies and responds to many of the issues raised in the Office of Inspector General (OIG) report.

CBP and USDA APHIS have forged a new working relationship and resolved many of the earlier port access issues. CBP, in conjunction with APHIS, has entered into several programs, such as the targeted program for imported cut flowers to apply inspection resources on a risk managed basis (i.e., focus on commodities that pose a higher risk to American Agriculture). Also, CBP and APHIS have worked together in numerous ways to synchronize and verify information and data collected

about inspections such as the Joint Quality Assurance Program, which provides a quality assurance team to conduct port reviews. CBP and USDA employees are working together cooperatively and sharing information. CBP has worked with USDA to achieve the appropriate level of access to the ports of entry for APHIS personnel. As Congress has provided, the inspectional functions were transferred from USDA to CBP. CBP has set forth procedures that have facilitated USDA access to the ports to perform their functions.

Question. The OIG report includes information of the lengthy time that was required to negotiate and sign official agreements between APHIS and Customs and Border Protection (CBP). Several of these have taken more than 12 months. Additionally, APHIS reported that attempting to elevate issues within the Department of Homeland Security was not productive due to high turnover in the policy-making levels of DHS. The Homeland Security Act of 2002 split the agriculture responsibilities between these two agencies. If this is not working, should this situation be reevaluated?

Answer. Section 421 of the Homeland Security Act of 2002 (the Act) transferred to DHS the inspectional functions of APHIS relating to agricultural import and entry inspection. By the provisions of the Act, the Secretary of USDA and the Secretary of DHS were required to execute a memorandum of understanding (MOU) to cover this transfer in more detail. The MOU was signed on February 28, 2003.

Under the provisions of the MOU, the two agencies would work out further details of this relationship by the means of appendices to particular articles in order to allow for the development of procedures that would work for both agencies. To date CBP and APHIS have signed appendices to all the articles except for Article 4 that involves training in order to allow for the development of procedures that would work for both agencies. The time spent in developing the correct procedures has been well worth the delay as the training functions between the two agencies are working effectively. A completed Appendix for Article 4 is expected to be signed in early summer 2005.

We have also developed procedures and mechanisms to work through issues as they arise in the future. The time taken to draft, negotiate and finalize these appendices has been a necessary part of a growing partnership between these two agencies. The organizational and functional task allocations are working. The agricultural program is being strengthened through training and cross training.

NATIONAL PREPAREDNESS GOAL

Question. The Administration released the Interim National Preparedness Goal (the Goal) on March 31, 2005. States are required to update their State Homeland Security Strategies, by October 1, 2005, with an assessment of what gaps remain in each state's ability to meet the tasks and capabilities laid out in the Goal. The proposal put forth by the fiscal year 2006 President's budget would prioritize Federal funding received by State and local governments for first responders not just by threat and vulnerability, but also by "essential capabilities" as defined in the Goal. Each State is required to file an addendum by October 1, 2005, to its State Homeland Security Strategy to reflect how it will address the seven national priorities. Is this enough time for the States to do a thorough evaluation of what capabilities each has now?

Answer. Yes, DHS believes that there is enough time for the States to complete a thorough evaluation of their current capabilities. Specifically, in fiscal year 2005, during year 1 of the implementation of Homeland Security Presidential Directive (HSPD) 8, States and urban areas are required to update their existing homeland security strategies. To meet this requirement, the Department is asking States and urban areas to review their existing strategic goals and objectives and bring them into alignment with the seven National Priorities outlined in the National Preparedness Goal by September 30, 2005. (The seven National Priorities are: (1) Implement the National Incident Management System and National Response Plan; (2) Expand Regional Collaboration; (3) Implement the Interim National Infrastructure Protection Plan; (4) Strengthen Information Sharing and Collaboration Capabilities; (5) Strengthen Interoperable Communications Capabilities; (6) Strengthen CBRNE Detection, Response, and Decontamination Capabilities; and (7) Strengthen Medical Surge and Mass Prophylaxis Capabilities.) This first step in HSPD–8 implementation will not require States or urban areas to conduct a wholesale rewrite of their strategies, nor will they have to complete another risk and capabilities assessment as they did in fiscal year 2003. DHS completed guidance on completing this strategy in June 2005. More detailed information on this requirement was presented to State and urban area representatives at three National Preparedness Goal rollout conferences throughout April and May 2005. Additional details are also available to

State and urban area representatives through their designated Preparedness Officers within the Office for Domestic Preparedness (ODP) in the DHS Office of State and Local Government Coordination and Preparedness (OSLGCP).

Question. An important aspect of the National Preparedness Goal has not been defined, the levels of capabilities for differently sized jurisdictions. How are Manchester, NH, and New York, NY, supposed to know what different types of capabilities that each should have for a chemical incident?

Answer. The Interim National Preparedness Goal establishes the national vision and priorities that will guide DHS' efforts, in conjunction with appropriate stakeholders, to set measurable readiness benchmarks and targets to strengthen the Nation's preparedness. The Target Capabilities List is a set of 36 essential capabilities that should be developed and maintained, in whole or in part, by various levels of government to prevent, protect against, respond to, and recover from terrorist attacks and major disasters. DHS, working with stakeholders, is currently developing national target levels for the capabilities and the role of Federal agencies, states, local jurisdictions, the private sector and non-governmental organizations in building and maintaining the network of capabilities across the country required for large-scale incidents. Local jurisdictions will be expected to build and maintain levels of capability appropriate to their risk. DHS has invited Federal agencies, State representatives, and national associations to participate in a series of workshops to set the target levels.

Question. How will you encourage States to be thorough in their assessment of their capabilities?

Answer. In out-year implementation of HSPD–8, States will be required to assess their current capabilities against target levels of capability that will be defined in the Target Capabilities List. However, in fiscal year 2005, the capability assessment will be conducted through a representative sampling of States and/or sub-state regions to test and validate the assessment process prior to nationwide implementation. As part of this representative sampling of capabilities, DHS will develop user-friendly tools based on the Target Capabilities List to ensure that both States and multi-disciplinary subject-matter expert teams conducting the assessments are thorough in their evaluation of capabilities. In addition, DHS will provide customized reports to States that link their existing capabilities and grant expenditure data to the National Priorities outlined in the National Preparedness Goal in order to assist States as they begin to implement HSPD–8.

Question. What is the incentive for a State to close a gap if doing so results in less funding for that State?

Answer. The Department believes there are sufficient incentives for States to build both regional and statewide capabilities and close identified gaps in overall preparedness. Enhanced preparedness to protect against, respond to, and recover from incidents of a national emergency, including terrorism, will ultimately result in minimizing the adverse impact on lives, property, and the economy that are inherent to a catastrophic event. The protection of citizens, critical infrastructure, businesses, and communities is a shared goal, requiring Federal, State, local, international, and private sector partnerships. Throughout the Nation, States are embracing this goal as the ultimate incentive, as they work to implement the National Preparedness Goal. Finally, the extent of "unmet gaps" will not be the sole determinant of DHS grant allocations.

Question. How exactly does the Administration envision this working?

Answer. The Interim National Preparedness Goal includes a vision, which is "to engage Federal, State, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy."

The Interim National Preparedness Goal and companion National Preparedness Guidance outline how the Nation will achieve this vision. The Guidance outlines a 10-step national process for Capabilities-Based Planning that will be used to identify target levels of capability, achieve them, and assess preparedness from the local to the national level. The Goal and Guidance establish seven National Priorities focused on developing some of the more critical capabilities from the Target Capabilities List for which the Nation is currently the least prepared (Information Sharing and Collaboration; Interoperable Communications; Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) Detection, Response, and Decontamination; and Medical Surge and Mass Prophylaxis) and overarching initiatives (to implement the National Incident Management System, National Response Plan, Interim National Infrastructure Protection Plan, and expand regional collaboration) that will facilitate those efforts. The Guidance highlights existing Federal program efforts that support the seven National Priorities and describes a schedule of activities for

States and urban areas to update assessments and strategies with Federal assistance.

The process is collaborative, iterative, and risk-based. Homeland security is a shared responsibility and depends upon shared efforts. This approach will be implemented through multi-agency and multi-discipline working groups at the national and regional (or multi-jurisdiction) level. Federal preparedness assistance will explore ways to offer incentives and rewards for collaboration. This approach involves a continuous cycle of activity to refine our assumptions and planning tools and share best practices and lessons learned. This approach recognizes that while all jurisdictions are subject to some degree of risk, the capabilities and levels of capability that are needed to manage risk vary considerably across the Nation. Annual status reports will provide a more meaningful assessment of national preparedness. Data collection will simplify over time as tools are refined and consolidated. This approach will provide a sound basis for decisions at all levels of government to allocate resources based upon risk and need.

Question. Will "essential capabilities" as defined by the National Preparedness Goal be considered equal to threat information, population density, or other factors?

Answer. The development of the target capabilities, or "essential capabilities," by Federal, State, local, and tribal entities and the private sector will be driven by relevant threat information, population size and density, critical infrastructure, and other factors. DHS is working with Federal, State, local, tribal, private sector, and non-governmental stakeholders to refine the Target Capabilities List (TCL) for reissuance on October 1, 2005. This new version of the TCL will assign the capabilities by level of government and tiers (groupings of local jurisdictions). The primary purpose of the tiers is to account for reasonable differences in target levels of capability (or system-specific elements of capability) among groups of jurisdictions based on differences in risk factors such as total population, population density, and critical infrastructure.

Question. Once a State obtains certain capabilities, how do we sustain that effort? Should the States be responsible for sustainment costs?

Answer. As we have barely begun to assess current capabilities, it is premature to speculate about future funding requirements once the most significant gaps are closed. While maintenance of effort will largely be State and local responsibility, DHS will continue to assist States in building and sustaining the target capabilities. Additionally, every State and locality will have a role in achieving and sustaining the 36 capability target levels. However, the target capabilities are a planning tool, not a funding formula. Implementing Capabilities-Based Planning is a long-term effort that will help the Nation to achieve the capacity to perform all 36 target capabilities at the levels needed to effectively prevent, protect against, respond to, and recover from major events, especially terrorism. Not until States and urban areas have assessed and realigned their homeland security strategies and plans will DHS be able to fully determine which of the 36 target capabilities will require additional funding.

FUNDING FOR FIRST RESPONDERS

Question. Just in the last few weeks national news reports have questioned the use of first responder grants in relation to homeland security. In January of 2005, the Department of Homeland Security Office of Inspector General issued a report questioning how the Department prioritized port security grants.

Given all of this, how confident are you that every dollar that has been allocated for homeland security grants has been well spent?

Answer. In general, homeland security port security grants have been well spent. Recognizing that issues emerged with some projects, the Department disagreed and non-concurred with the IG's finding that projects received funding despite ranking "average to worse" during the evaluation process. Following TSA's second round of grant awards in 2003, ODP made $75 million available for port security grants under the Urban Areas Security Initiative (UASI). ODP, in consultation with TSA and SLGCP, utilized a risk-based approach, which differed from the program's original competitive process to select 14 eligible port areas and the corresponding funding amounts for each area. TSA then provided unfunded applications from its second round to ODP, which in turn, funded 86 projects. TSA provided what they considered to be the next projects that had been evaluated from the previous round that deserved funding. All of the 86 projects were funded based on TSA's recommendations.

The Department has made significant efforts to improve the Port Security Grant Program in light of the Inspector General's (IG) report. The report recommended that the Department accelerate the acquisition of more information from applicants

about the scope of their projects in an effort to expedite the spending of grant awards. We concur with this recommendation and will ensure that appropriate guidance on the submission of relevant information within specified timeframes is included in the application kit for the forthcoming fiscal year 2005 Port Security Grant Program. Additionally, the IG report recommended that the Department ensure that the program has sufficient operational expertise to administer the program after the award is made. We concur with this recommendation as well, and have established a Transportation Infrastructure Security Division (TISD) within SLGCP to administer the fiscal year 2005 Port Security Grant Program. Given the reforms in response to the IG report, DHS port security grants will be managed even more effectively under the fiscal year 2005 Port Security Grant Program. Additionally, SLGCP has developed mechanisms intended to increase accountability of all grant programs, an effort recognized in a recent GAO Report entitled, "Management of First Responder Grants Has Improved, but Challenges Remain" (#05–121).

Question. The Senate and the House Appropriations Committees asked for a report on homeland security grant spending. This report is to include information on what has been purchased with all of the grant dollars from fiscal years 2002 through 2004, whether these purchases complied with the State Homeland Security Strategies, and an explanation as to how this spending has enhanced the Nation's security. That report was due March 31, 2005, but it has not yet been submitted. When can we expect it?

Answer. The congressional report on "State and Local Government Preparedness and Funding for Fiscal Year 2002-Fiscal Year 2004" was delivered to the House and Senate Appropriations Committees on May 6, 2005.

Question. If the Department goes to a completely threat-based formula, are you comfortable with how threats are determined now? I know we can't talk in detail in an open forum—but what, if anything, would you change?

Answer. The President's fiscal year 2006 Budget proposes a risk-based homeland security funding process, of which threat is one component along with consequence and vulnerabilities. DHS will consider risk factors such as threat, presence of critical infrastructure, vulnerability, population and population density, international borders, and ports of entry in making final award determinations. This process will be modeled on the fiscal year 2005 UASI program, which combined five variables designed to objectively prioritize funding for high-threat, high density urban areas. A threat estimate index developed from an estimate of credible threats and incidents as well as an index that considered law enforcement investigative activity and enforcement will be used. The difficulty of determining which States and urban areas most are at risk is subjective to some degree because of the nature of most intelligence information and the scarcity of data specifically identifying targeted states, cities and infrastructure. Therefore, the current allocation methodologies that consider threat information represent the best available combination of data, current understanding of threats, and expert judgment.

Question. What restrictions are placed on the use of these grant funds?

Answer. DHS released detailed guidance for the use of grant funds contained in the fiscal year 2005 Homeland Security Grant Program (HSGP). Specific guidelines on intended purpose and the allowance of certain types of expenditures vary between the six different programs contained in the HSGP. HSGP allowable costs are divided into planning, organization, equipment, training, and exercise categories. Management and administrative and certain operational costs are also allowed under certain programs. Allowable equipment categories for the fiscal year 2005 HSGP are listed on a web-based Authorized Equipment List on the Responder Knowledge Base, which is sponsored by ODP and the Oklahoma City National Memorial Institute for the Prevention of Terrorism at http://www.rkb.mipt.org.

The fiscal year 2005 HSGP guidance also details certain restrictions placed on the use of grant funds, which vary by program. For example, funding in the UASI and Law Enforcement Terrorism Prevention Program programs may not be used for overtime to supplant ongoing, routine public safety activities of State and local emergency responders, and may not be used to hire staff for operational activities or backfill. However, these programs do allow up to 25 percent of the awards to be used for operational expenses and overtime for periods of heightened alert, for personnel to participate in information, investigative and intelligence sharing activities related to homeland security, and finally, in the hiring of contractors/consultants for participation in information/intelligence sharing groups. Another example of restriction on funds involves construction and renovation. Use of HSGP funds for construction is generally prohibited and is allowable only when it is a necessary component of (1) a security system at critical infrastructure facilities or (2) an emergency operations center (EOC). Details on other restrictions for certain types of equipment, training, and exercises are provided in the fiscal year 2005 HSGP guidance.

Question. What audits have been done, or are underway, to ensure that these grant funds are used appropriately? What other controls does the Department have at its disposal to oversee the use of grant funds?

Answer. During calendar year 2004, SLGCP was a part of over 14 governmental audits, ranging from the Government Accountability Office (GAO) to the DHS Inspector General to the House Appropriations Survey & Investigations Staff (S&I). Many of these audits looked at the expenditure of grant funds by the States and territories. Some of these audits have provided final reports, and most of those reports reflect SLGCP's ability to efficiently process the grant, as well as provide programmatic assistance and oversight to the states. A recent GAO Report entitled, "Management of First Responder Grants Has Improved, but Challenges Remain" (#05–121) credits SLGCP with developing requirements intended to hold States and localities accountable for how grant expenditures were planned, justified, expended, and tracked.

In order to assure fiscal and programmatic oversight, ODP Preparedness Officers have robust monitoring and reporting tools through which they can monitor expenditures by grantees. The Initial Strategy Implementation Plan and the Biannual Strategy Implementation Report provide detailed expenditure information by discipline, solution area (such as equipment or training) and project area. These reports require grantees to tie any expenditure of homeland security funds to goals and objectives outlined in their State or Urban Area Homeland Security Strategy. They also provide important data on what projects are being accomplished by States and localities. In addition to the almost daily contact with grantees, Preparedness Officers also perform a formal on-site monitoring visit to their States at least once a year, in accordance with program office protocols. This visit allows for both programmatic and financial compliance monitoring. The Department of Justice's Office of the Comptroller (OC) also performs random, risk-based financial audits of SLGCP grantees. Each State Administrative Agency (SAA) also is subject to its own State audits. The combination of these external and internal inspections provides the required oversight over the use of SLGCP grant funds.

INTEROPERABLE COMMUNICATIONS

Question. The Federal Government has been working for many years to crack the nut of moving more quickly towards true interoperability. Do you see the creation of the Office of Interoperability and Compatibility as helping move towards that goal? Is this just another Office that will put forth a lot of effort and get very little advancement?

Answer. The Science and Technology (S&T) Directorate's Office for Interoperability and Compatibility (OIC) has made significant achievements in helping the Federal Government move more quickly towards interoperability. The OIC was created to address critical interoperability issues relating to public safety and emergency response, including communications (the SAFECOM Program), equipment, training and other areas as needs are identified.

Since its inception OIC has:

—Released Version 1.0 of the first ever comprehensive Public Safety Statement of Requirements (SoR) for Communications and Interoperability (SoR), which defines the functional requirements for public safety practitioners to communicate and share information when needed, where needed, and when authorized.

—Developed the Interoperability Continuum, a tool designed to help the public safety community and local, tribal, State, and Federal policy makers address critical elements for success as they plan and implement interoperability solutions. The critical elements include governance, standard operating procedures, technology, training/exercises, and usage of interoperable communications.

—Created the Statewide Communications Interoperability Planning (SCIP) Methodology, based on lessons learned from assisting the Commonwealth of Virginia in developing a strategic plan for improving statewide communications interoperability. The SCIP Methodology serves as a guide for States to consider as they initiate statewide communications planning efforts.

—Developed coordinated grant guidance which provides the public safety community with consistent guidance, coordinated application processes, similar requirements across grant programs, and general guidelines for implementing a successful wireless communications system. This guidance was incorporated in the fiscal year 2003 FEMA and fiscal year 2003/fiscal year 2004 Community Oriented Policing Services (COPS) grant awards, as well as ODP grant packages in fiscal year 2004.

—Drafted a report as required by the Intelligence Reform and Terrorism Prevention Act that discusses DHS plans for accelerating voluntary consensus standards for interoperable communications.
—Managed the RapidCom initiative, in which the Office worked with ten urban areas to provide requested assistance to help improve incident level interoperability capabilities and developed a methodology for a communications table top exercise that is replicable across urban areas.
—Awarded a contract to develop and execute the nationwide interoperability baseline study in January 2005. The purpose of the study is to quantify the extent to which the Nation's public safety first responders are interoperable technically and operationally.

With respect to other critical interoperability issues, the OIC has done the following:

—Created the Risk Assessment Policy Group (RAP) from representatives within DHS to address and resolve discrepancies in risk assessment criteria and methodologies. RAP hosted a workshop with stakeholders from the Department to clearly define the scope of the risk assessment problem and to develop a strategy for addressing the problem.
—Created the Joint Evaluation and Testing Program (JET) to coordinate Federal programs that conduct testing and evaluation of public safety technologies. JET hosted a planning meeting with representatives from DHS, the National Institute of Standards and Technology, and the Department of Justice to define the scope of the JET program.

Question. The Office of State and Local Government Coordination and Preparedness reports that in fiscal year 2004 more than $890 million of the grants given to States and locals were used in some way for interoperable communications, equipment, studies, etc. What is being done to help States and locals today to make better decision about investments in interoperable communications?

Answer. SLGCP has leveraged the S&T Directorate's SAFECOM program's development of standards and grant guidance to help create the Interoperable Communication Technical Assistance Program (ICTAP). ICTAP is a technical assistance program designed to enhance interoperable communications between local, State, and Federal emergency responders and public safety officials. The goal of the ICTAP program is to enable local public safety agencies to communicate as they prevent or respond to a WMD attack. The ICTAP program provides free, on-site support using a systems engineering approach. The ICTAP technical assistance team works closely with the UASI site's Urban Area Working Group to assess the current communications infrastructure for gaps and to translate operational requirements into technical requirements that can be used to design an interoperable communications system.

AIR CARGO SECURITY

Question. Does the Transportation Security Administration (TSA) have any cost estimates for screening 100 percent of the baggage and cargo on passenger planes?

Answer. The total amount of cargo transported on passenger aircraft represents less than 25 percent of the total air cargo volume transported in the United States. TSA completed a study in 2002, "The Air Cargo Security Scenario Analysis Report," that indicated that the cost of screening 100 percent of the cargo transported on passenger aircraft at the top 42 airports, which handle 95 percent of the total volume of air cargo transported in the United States, would cost $500 million in the first year and $3.8 billion over 10 years.

Question. Though you cannot deter every threat, do you believe 100 percent screening of high-threat of bags and cargo is the best use of our Federal resources?

Answer. TSA has taken a threat-based, risk-managed approach to air cargo screening. This approach helps the agency appropriately target screening efforts with the resources available. TSA believes that all cargo should be pre-screened for risk through the Known Shipper Program or the Indirect Air Carrier Program, and that 100 percent of cargo that is identified as elevated-risk should be screened using appropriate technology and methods. Random inspections play an important, complementary role in the layered systems approach by managing risk without unduly impeding the flow of commerce.

Currently all cargo that will be transported on passenger aircraft is pre-screened for risk through the Known Shipper Program. Passenger air carriers, Indirect Air Carriers (IACs, or freight forwarders), and all-cargo carriers who transfer cargo to passenger planes all use the Known Shipper Program. TSA's Known Shipper Database has centralized the collection of data on about 450,000 known shippers and enabled vetting against government databases. To supplement the Known Shipper

pre-screening, air carriers are also required to conduct random screening of a certain percentage of air cargo.

In 2005, TSA has developed an Air Cargo Security Roadmap that integrates many policy, operations, system, and regulatory enhancements to air cargo security. The cornerstone of this effort is the Freight Assessment System (FAS), which would enable TSA to better and more efficiently identify elevated-risk cargo for inspection. FAS will employ a sophisticated risk assessment engine to identify elevated-risk air cargo for inspection.

Additionally, TSA has published a robust Notice of Proposed Rulemaking (NPRM) for air cargo security. This NPRM is currently being developed into a final rule, which implements major security enhancements for indirect air carriers (IACs), all cargo carriers, passenger carriers, and airports.

Finally, TSA oversees compliance with security requirements through a robust regulatory compliance program, which includes more than 900 aviation security inspectors located throughout the United States.

Question. How can we better tackle the issue of cargo security?

Answer. TSA continues to make incremental and measured progress in the air cargo arena, among other things by prohibiting cargo from unknown shippers, significantly increasing the number of physical inspections of air cargo on passenger and all cargo aircraft, increasing its air cargo inspections workforce, strengthening the criteria for consideration as a known shipper, automating the validation of known shippers and indirect air carriers, and expediting research and development efforts to identify potential new technological solutions for the inspection of air cargo on passenger aircraft. TSA is also working closely with CBP to develop a targeting tool which will permit effective identification of elevated risk cargo with the ultimate goal of requiring the inspection of all such elevated risk cargo.

Question. What is the right mix of screeners and technology when dealing with air cargo and how does the Department determine which resources to apply?

Answer. TSA has taken a threat-based, risk-managed approach to air cargo screening. This approach helps the agency appropriately target screening efforts with the resources available. TSA believes that all cargo should be pre-screened for risk through the Known Shipper Program or the Indirect Air Carrier Program, and that 100 percent of cargo that is identified as elevated-risk should be screened using appropriate technology and methods. Random inspections play an important, complementary role in the layered systems approach by managing risk without unduly impeding the flow of commerce.

TSA employees do not conduct the screening of air cargo. Rather, the screening is performed by air carriers and overseen by TSA. TSA issues regulatory requirements to air carriers in this area, and TSA's inspectors provide oversight and work to ensure that carriers are meeting their regulatory requirements.

Question. What other means is TSA using to achieve more secure cargo-holds in passenger carriers?

Answer. TSA is continuing efforts to design blast resistant cabin and cargo liners, as well as overhead bin mitigation technological solutions. The agency has completed initial feasibility studies for both passenger cabin and cargo hold liners. The results of the studies are promising. The agency is working on preliminary designs, and a prototype is expected by the end of calendar year 2005. TSA is also partnering with the FAA and aircraft manufacturers to determine which solutions are best suited for retrofitting existing aircraft with this new technology.

Additionally, TSA is conducting a pilot program to evaluate the use of blast-resistant containers for cargo and baggage on passenger aircraft to fulfill the requirements of Section 4051 of Public Law 108–458, the Intelligence Reform and Terrorism Prevention Act. The objective of the hardened unit load device (HULD) pilot program is to determine the feasibility, including operational impact, durability, cost, maintenance, training, blast containment, and logistics, of an HULD solution. The pilot program began in June 2005, and the data collection will last approximately 18 months from the start date.

Question. How difficult is it for TSA to secure the air cargo processing "footprint" at the airports from the time of entry into the system maintaining a chain of custody until the moment of its loading onto a plane?

Answer. Regulated airports already secure their air cargo processing "footprint" through security measures specified within their airport security program which identifies a portion of the airport as Secured Area, Security Identification Display Area, and Sterile Area. These security procedures are designed to prevent unauthorized entry, presence, and movement of individuals and ground vehicles within the air operations area. Current procedures require a personnel identification system which allows different levels of access, subjects individuals to employment history verification checks, and provides individual training.

Question. What are other countries doing to address this issue?

Answer. The United Nations' International Civil Aviation Organization (ICAO) establishes International Standards, Recommended Practices and Procedures covering the technical fields of aviation, including air cargo security.

Countries or States, as commonly referred to by ICAO, are afforded a great deal of discretion to establish and implement measures to comply with standards directly related to air cargo security. The substance of ICAO's air cargo standards are as follows:

—States shall ensure the implementation of measures at airports serving international civil aviation to protect cargo and baggage moved within an airport and intended for carriage on an aircraft to safeguard such aircraft against an act of unlawful interference.

—States shall establish measures to ensure that cargo intended for carriage on passenger flights are subjected to appropriate security controls.

—States shall establish measures to ensure that operators do not accept consignment of cargo for carriage on passenger flights unless the security of such consignments is accounted for by a regulated agent or such consignments are subjected to other security controls.

The ICAO Security Manual provides guidance on how an ICAO Member State might comply with the standards. The methods of compliance provided in the guidance material are based on generally recognized practices and procedures common within the international civil aviation industry, but they are not the only means of compliance. ICAO recognizes that other methods of compliance may be equally appropriate.

TSA PASSENGER FEES

Question. The President's budget request proposes increasing the passenger security fee by $3.00 from $2.50 to $5.50 for the first leg of an airline trip. Has TSA or the Department conducted any studies to determine what the flying public would pay in exchange for better aviation security?

Answer. Yes. The Aviation and Transportation Security Act (ATSA), enacted in November 2001, anticipated that the aviation industry, not the general taxpayer, would pay for airline security costs. To estimate the passengers' willingness to pay the additional cost of air transportation, TSA conducted an analysis that included comparing year-to-year revenue collections, reviewing Department of Transportation data reported by the airlines themselves to estimate industry growth, utilizing the Federal Aviation Administration's (FAA) aviation industry forecast, and accessing major research studies that outline issues from airline fare structure to passenger demand and willingness to pay.

TSA also conducted a review of current research on air passengers' willingness to pay for aviation security. Of particular interest to TSA was a survey conducted by the National Opinion Research Corporation in August 2002 of airline passengers for the American Automobile Association (AAA). In that survey, approximately nine out of ten respondents indicated that they were willing to pay something more than the current passenger security fees. AAA's conclusion is as follows: "Americans remain committed to aviation security. It's one thing to demand increased security and to be unwilling to pay for it. No one likes to pay more for the goods or services we buy. But what this survey seems to say is that Americans not only want to feel secure when they fly, they are willing to pick up some of the cost, if necessary."

Question. What is the impact to the industry?

Answer. TSA believes that the modest fee increases of this proposed budget should not undermine passenger traffic nor worsen the industry's health. U.S. air traffic reported for 2004 by the Department of Transportation (DOT) is near or above the year 2000 levels. Despite the re-imposition of fees after a 4 month suspension under the Emergency Wartime Supplemental Appropriations Act, 2003 (Public Law 108–11), the DOT domestic passenger traffic statistics showed an increase from a total of 588 million in 2003 to 630 million in 2004—a 7.2 percent increase.

TSA researched the impact the fee increase might have on airline profitability. TSA was unable to locate any study that conclusively linked a passenger fee increase, applicable to all airlines, with a measurable decline in airline profitability. The September 11 Security Fee is a uniform fee imposed on the passengers of all similar air carrier operations and flights. Consequently, the fee should not put individual airlines in a competitive disadvantage with one another. In fact, the security and other aviation fees comprise a larger percentage of the ticket price for low cost carriers, yet the low cost carriers are currently the most profitable among the domestic airlines.

TSA regularly monitors the state of the aviation industry, including the level of operations and the financial status of the airlines. Here are two examples of informational sources TSA uses in order to accomplish this goal:

—Various publications of the DOT Airline Fares Consumer Report were analyzed, and it was found that the answer depends upon various factors such as market size, number of carriers, and market structure. The data shows that competition within the aviation industry has a stronger influence on base fares than security fees.

—Canada has extensively researched the economic impact of its passenger security fee called Air Travelers Security Charge. Using both Canadian and U.S. data, the researchers concluded that markets with traffic levels over 100,000 passengers are relatively price inelastic (an increase in price results in either no or virtually no reduction in demand.). The research results did not find that the September 11 Security Fee impacts airline profitability.

Question. Does the passenger fee proposal require legislation or are there other options?

Answer. The passenger security service fees were authorized by the Aviation and Transportation Security Act and codified at 49 U.S.C. 44940. Currently, 49 U.S.C. 44940(c) limits the passenger fee to $2.50 per enplanement, not to exceed $5 per one-way trip. The proposal to increase the passenger fee would require 49 U.S.C. 44940(c) to be modified to set the new fee level at $5.50 per enplanement, not to exceed $8 per one-way trip.

Question. The budget requests that this fee change be legislated on an appropriations bill. However, this should properly be submitted to the authorizing committees of jurisdiction. Has the President transmitted the proposed legislation to Congress for consideration and if not, why?

Answer. The President provided a legislative proposal to modify this fee authority in the fiscal year 2006 budget. In Title V—General Provisions of the Appendix (page 526), the proposal states: "SEC. 517. In Chapter 449 of title 49, United States Code, section 44940(c) is amended by striking '$2.50' and replacing it with '$5.50', and striking '$5.00' and replacing it with '$8.00'." This modification to the fee authority would allow TSA to implement the fee increases sought in the President's fiscal year 2006 Budget.

Question. What will be the impact on DHS' programs and activities if this legislative proposal is not enacted as a general provision of the Appropriations Act or by the appropriate authorizing committee?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

Question. When would such a fee request have to be enacted to fund fiscal year 2006 activities?

Answer. TSA estimates that if the fee were to be enacted in time to be effective at the beginning of fiscal year 2006, the agency will be able to raise as much as $1.879 billion in additional fees. If the proposal is enacted after October 1, the delay involved in providing the necessary updates in fees and guidance to the industry could result in reduced collections.

Question. What new aviation security measures would you put in place utilizing the increased revenues or will these resources be used throughout the Department?

Answer. The purpose of the fee increase is not to fund new activities. Rather, it is to offset funding from the general fund with fee revenue. Compared to the past and current level of 50 percent or less, the fee would contribute to offsetting nearly the full amount of TSA screening costs.

These costs represent the vast majority of TSA's aviation security screening costs. TSA does not have the authority to offset any other costs with the aviation security fee collections. The increased fees on passengers, the users of the security screening, will ensure fee levels approaching near full recovery of the Federal cost to operate the system.

TSA AIR CARRIER SECURITY FEES

Question. At the direction of the Committee, GAO has completed a review in order to validate the air carrier's estimates of their security costs in 2000. GAO found that the estimates, currently the foundation for the fees paid to the Department by the airlines, are $127 million too low. Due to these findings, Mr. Secretary, will you take action to collect the additional fees from the airlines?

Answer. In the Homeland Security Appropriations Act, 2005, (Public Law 108–334) Congress directed the GAO to determine how much air carriers spent on security screening in 2000—the basis for the fee imposed on airlines. GAO completed its review and issued a report on April 18, 2005. The report concludes that the amount of the industry-wide passenger and property screening costs was between $425 million and $471 million, with a midpoint estimate of $448 million. The midpoint difference between what is collected now and what GAO indicates should be collected is $129 million. However, GAO's estimate did not include certain cost categories (e.g.; real estate, CAPPS, and positive bag match) due to the unavailability of information within the timeframe provided. The cost of these items could be significant. TSA is currently reviewing all the findings of the. Once TSA completes its review, the agency will proceed as quickly as practicable to address the issue.

Question. Will TSA require legislation to change the air carriers' charges or can this be done through regulation?

Answer. No legislation is required. The fiscal year 2005 Homeland Security Appropriations Act and the Aviation and Transportation Security Act, as codified at 49 U.S.C. 44940, provide sufficient authority for TSA to collect additional amounts from the air carriers. However, changes to the air carriers' fees would require changes to regulations currently in effect at 49 CFR Part 1511.

Question. When must the regulation be in place in order to generate enough revenues to cover your costs in fiscal year 2006?

Answer. To collect the air carrier fee at the current level of approximately $315 million in fiscal year 2006, no new or changes in the regulation would be required. The $350 million estimated in the President's budget captures costs that are currently disputed or not reported altogether by air carriers due to bankruptcies. TSA is in the process of pursuing the amounts under dispute. The unreported and disputed costs will be determined and charged when TSA implements the new structure for the air carrier fee, for which rulemaking is currently in progress. Additionally, TSA is currently reviewing GAO's findings that the aviation security costs self-reported by the air carriers should be $448 million, $129 million more than originally reported by the industry.

Question. Will your regulatory proposal focus on changing the basic structure of how airlines are charged for security costs or is it intended to focus on the difference between the actual revenue generated, $350 million, and TSA's target last year of $750 million?

Answer. TSA is evaluating the current regulatory approach to determining if change is needed.

Question. For fiscal year 2005, there are some that estimate the air carrier fee will generate only $315 million, not $350 million. What are you planning to do to address any shortfall?

Answer. The $315 million represents a total rounded year 2000 cost figure reported by all carriers to TSA. The $350 million estimate captures costs that are currently disputed or not reported altogether by air carriers due to bankruptcies. TSA is in the process of pursuing the amounts under dispute. The unreported and disputed costs will be determined and charged when TSA implements the structure for the air carrier fee, for which rulemaking is currently in progress.

Question. What activities will go unfunded or deferred as a result of the funding gap?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

TSA CONTRACT SCREENERS

Question. What analysis has the Department done to determine whether contracting for private screeners is cost-effective and equally or more effective in terms of security than a federalized force?

Answer. TSA commissioned an independent evaluation of the five pilot airport passenger screening programs that was completed in April 2004. The evaluation utilized a methodology that included the following:

Evaluation Categories:

—Security effectiveness: covert test results, Threat Image Protection (TIP), and re-certification scores;

—Customer/stakeholder satisfaction: customer surveys, stakeholder surveys, and customer complaints; and

—Cost: total cost the contractor charged for screening services (including only contract payments and costs borne by TSA) compared to estimates on how much would have been spent by TSA had the agency conducted the screening operations at those airports.

The evaluation concluded that there was no statistical difference in any of the three evaluation categories between private and Federal screeners. In addition, as more airports transition to the Screener Partnership Program (SPP), TSA plans to continue to measure costs of Federal screening operations compared to private screening companies.

TSA also commissioned an activity-based cost (ABC) study to provide improved visibility into the costs of specific business processes and activities, and the associated resources (e.g., people, technology) consumed by those processes and activities (i.e., cost per bag or person screened). The ABC study included ten randomly selected airports that utilize TSA screeners and the five pilot airports. The study will better enable TSA to identify and collect the cost and performance metrics needed to establish a successful, ongoing cost and performance management framework at TSA. The results of the ABC study will provide another means for TSA management to assess screening operations by airport.

Question. Is TSA establishing a cost benchmark and collecting the right kind of information in order to evaluate the costs of providing Federal screeners vs. the costs of having contract screeners?

Answer. TSA plans to develop a cost baseline for each airport that applies to participate in the SPP. This cost baseline will be used to evaluate cost proposals from private screening companies. The results of the TSA activity-based cost study will also support development of these baselines.

Question. In what ways is it more effective for the government to use contract screeners?

Answer. An independent evaluation concluded that there was no statistical difference between private and Federal screeners. TSA believes that the independent evaluation, along with the activity-based cost study, confirms that TSA has been successful in administering an effective private screening program that is capable of providing security screening services at levels required by the ATSA.

Question. What incentives do you have in place and what are you doing to address the private sector's concerns about security liability related to the private screener workforce?

Answer. In directing TSA to establish a contract screening pilot program (PP5), the ATSA required that the level of screening services and protection provided at the PP5 airports be equal to or greater than the level provided at an airport with Federal screeners. Consequently, as airports consider whether to continue with Federal screening or to apply to the SPP, their decisions can be based on their own preferences and criteria rather than considerations of security, resources, or level of service.

ATSA states that TSA shall allow an airport operator to submit an application to have screening carried out by the screening personnel of a qualified private screening company. TSA is committed to developing a fair, balanced program that does the following:

—Meets ATSA standards
—Ensures security
—Seeks to establish a strong public/private partnership
—Provides significant opportunity for innovation, efficiency, and cost savings to the taxpayer
—Provides decentralized management
—Incorporates best practices and lessons learned from recent studies of the Pilot program, and continues to evaluate and learn on an on-going basis
—Is performance-based
—Does not restrict airport participation
—Respects Federal and private sector workforces

Under ATSA, the decision to apply for private screening services lies with individual airport operators. However, should TSA approve the application, TSA will continue to oversee airport security, whether an airport has private contract screeners or Federal screeners.

TSA does not provide specific liability limitations for private passenger and baggage screening services. However, vendors can apply for protections under the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). Enacted as part of the Homeland Security Act of 2002, the SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating a system of risk and liability management. The purpose of the Act is to ensure that the threat of liability does not deter potential manufacturers/sellers from mak-

ing anti-terrorism technologies available. The Act provides two types of benefits: (1) Designation as a Qualified Anti-Terrorism Technology ("QATT"), which among other benefits limits the seller's liability to the amount of available insurance, and (2) Certification as an Approved Product for Homeland Security, which allows the seller to assert the Government Contractor Defense. Sellers must apply for SAFETY Act protections and are evaluated in accordance with the statutory criteria. Protections under the SAFETY Act only apply when a QATT has been deployed in defense against, response to, or recovery from an act of terrorism. The Act contains a very broad definition of technology, which includes both tangible products and services as long as they designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring act of terrorism.

TSA is working with the S&T Directorate, which is charged with making determinations regarding the SAFETY Act. TSA understands that two of the private contract screening companies under the PP5 program have been granted designation under the SAFETY Act. TSA will also continue to work closely with DHS and the S&T Directorate regarding any decision DHS makes concerning the potential legal exposure of all entities participating in the Screening Partnership Program.

Question. How well have the privatized screeners at the 5 pilot airports worked?

Answer. TSA believes that private screeners and Federal screeners perform equally as well in screening passengers.

Question. A recent article in Government Security News reports that the traveling public is more satisfied with the private screeners than the Federal screeners. Is this an accurate statement?

Answer. This is not an accurate statement. TSA's annual customer service survey showed that for the second year in a row there was very little difference in the high degree of confidence and satisfaction air travelers have in TSA-trained screeners—Federal or private. For the second year in a row, air travelers gave consistently high marks to TSA's security screeners. Between 80 and 95 percent of passengers gave positive responses when asked about seven aspects of the Federal security screening process, which included thoroughness and courtesy of screeners as well as confidence in TSA's ability to keep air travel secure. In addition, TSA is meeting or exceeding passenger expectations for security line wait times.

Question. This past November TSA opened the Program Management Office to assist airports in privatizing their screener workforce. How many applications for private screeners has this office received?

Answer. As of May 2005, TSA has received seven applications from airport operators seeking to participate in the SPP. All five of the airports that participated in the private screening pilot program (PP5) have applied (San Francisco, Kansas City, Rochester, Jackson Hole, and Tupelo), along with two new airports (Elko, Nevada and Sioux Falls, South Dakota).

Question. How many applications for private screeners at airports do you anticipate receiving?

Answer. The decision on whether to apply to the SPP rests solely with the airport. Therefore, although several airports have expressed interest in participating in the program, TSA cannot speculate on how many will actually apply.

Question. How did you determine the level of screening service to be provided at these 5 airports?

Answer. The ATSA requires that the level of screening services and protection provided at the PP5 airports be equal to or greater than the level provided at an airport with Federal screeners. TSA will continue to set one standard for security for the entire commercial aviation system, whether an airport has Federal screeners or private screeners. TSA will ensure that standards are met through TSA security protocols, extensive contract oversight, conducting covert testing, and continuous oversight by Federal Security Directors and their staff in both Federal and SPP airports.

Per ATSA, TSA is also required to supervise private screening services at each SPP airport. Private screeners must perform at the same or better level as Federal screeners and comply with Federal passenger and baggage screening standard operating procedures.

ATSA also gives TSA the ability to terminate a contract with a private screening firm for repeatedly failing to perform. TSA will not hesitate to take action against airports using contract screeners if they fall below Federal security standards, and TSA will vigorously enforce the contract requirements.

Question. Are the screening standards for the privatized airports negotiated or does TSA establish them?

Answer. TSA applies the same rigorous security standards, referred to officially as Standard Operating Procedures, to private screeners as it does to the Federal screeners. Passenger and baggage security screening standards are non-negotiable.

Question. Does the contract include paying for the annual recertification of screeners by the contractor as well as compensation and benefits?

Answer. Yes. Screener annual re-certification training is conducted by and paid for by TSA. Private screener compensation and benefits are also funded by TSA up to the point required by the ATSA which mandates that private screeners receive compensation and benefits are not less than the compensation and benefits for Federal screeners.

Question. Does the private screener workforce have access to Federal benefits or is this just strictly a contract for services provided?

Answer. No, private screener workforce employees do not have access to Federal benefits. While the ATSA mandates that private screeners receive compensation and benefits that are not less than the compensation and benefits for Federal screeners, those benefits are not provided by the Federal Government. Screeners employed by private screening companies do receive benefits, and TSA monitors the overall pay and benefits package provided by private screening companies to ensure that the ATSA-mandated minimum is attained.

Question. What changes would you recommend to the contract screener program?

Answer. At the present time, TSA is not seeking changes to the ATSA regarding provisions to this program. TSA is open to and welcomes dialogue with airports and Congress on any improvements that could be made to the SPP. Some of the changes airports have indicated that they would like to see include the following:

—Change ATSA's requirement that private screening compensation and benefits be equal to or greater than Federal compensation and benefits

—Allow airports to share in any savings realized. For example, cost savings realized at an airport with private screeners would be used to enhance security screening at that airport

—Investigate pooling worker's compensation insurance to reduce costs through economies of scale

—Investigate broadening the private screening contractor's scope of responsibility to include other non-screening functions that impact security screening (e.g., document checkers, baggage handlers, bin runners, equipment maintenance, etc.)

TSA SCREENER TRAINING

Question. How many hours of training does the average screener receive?

Answer. The ATSA requires that all screeners complete a minimum of 40 hours of classroom training and 60 hours of On-the-Job (OJT) training. In addition to this basic training requirement, TSA Federal Security Directors (FSD) also use a standard of 3 hours per week (measured on average over a calendar quarter) of scheduled duty time, per screener, to accomplish recurrent, administrative, and professional development training. The FSD must create a training schedule that meets the goal of the 3 hours per week standard as well as the specific performance and developmental needs of each individual screener. In addition, TSA provides screeners with additional skills directly related to specific screener duties. An example is the On-screen Alarm Resolution Protocol (OSARP) Training. OSARP allows screeners to evaluate items causing an alarm and to potentially clear those items without subjecting the bag to a secondary search. The training for OSARP totals 19.5 hours and includes classroom training, small group simulator training, hands-on individual simulator training, and OJT training.

Question. Who conducts the training?

Answer. Basic screener training is overseen by TSA's Office of Workforce Performance and Training (WPT). The training is provided by instructors under contract with TSA or by local TSA Approved Instructors (TAIs) when possible. On-the-Job, cross-over, recurrent, and specialized training is conducted by local TSA personnel (i.e., TAIs, Training Coordinators, Screener Supervisors) and via the Online Learning Center. Advanced training is initially provided by WPT contractors and then sustained by TAIs.

Question. Does this training include anything regarding ethics and baggage theft?

Answer. During the initial 100 hours of basic training, TSA requires all screeners to review and sign a Code of Conduct. This Code of Conduct emphasizes such issues as public trust and honesty. Once initially trained, screeners continually receive recurrent professional ethics training including the "Customer Service Web-Based Training," which reinforces TSA's customer service principles and gives the screener training in various scenarios requiring effective customer service responses. Screeners are also provided the "TSA Pledge to Travelers," which emphasizes TSA's dual mission of providing World Class Security and World Class Customer Service, assures the traveling public that they are entitled to a security screening experience

that is professional and courteous, and that any experience to the contrary should be reported back to TSA. In addition, TSA has sent several communications to all employees (not just screeners) of their responsibilities on ethical conduct, including the restrictions under the Hatch Act related to the acceptance of gifts by Federal employees. All employees also receive a copy of and are required to sign TSA HRM Letter No. 735–1, Interim Policy on Employee Responsibilities and Conduct, which contains many of the Standards of Conduct provisions. Finally, to remind screeners of the consequences of unethical behavior, TSA has disseminated Management Directive 1100.75–3 informing screeners of the policies and procedures for disciplinary actions that could be taken against them.

TSA is committed to providing comprehensive ethics training and is currently developing a general ethics course that is expected to be available via the Online Learning Center by the end of the third quarter of fiscal year 2005. This course will cover topics such as principles, misuse of position, gifts, and outside activities.

Question. What is your response to the OIG's report regarding baggage theft by screeners?

Answer. TSA's responses to the specific recommendations in the Inspector General's report are as follows:

Recommendation 1.—Evaluate the adequacy of supervision, the physical layout of inspection stations, and the feasibility of installing electronic surveillance techniques near inspection stations.

TSA continuously reviews procedures related to the screening of baggage including supervision of personnel, physical layout, and electronic surveillance techniques. The agency will continue to do so by implementing the congressional requirements of the Intelligence Reform and Terrorism Prevention Act concerning checked baggage screening area monitoring, which requires the Under Secretary for Border and Transportation Security to provide assistance, subject to the availability of funds, to public airports that have baggage handling areas that are not open to public view in the acquisition and installment of security monitoring cameras for surveillance of such areas in order to detect theft from checked baggage and to aid in the speedy resolution of liability claims against TSA.

TSA's Office of Aviation Security Programs is working closely with the Office of the Chief Information Officer to plan and execute a program for the installation of electronic surveillance systems (ESS) to deter and detect incidents of baggage pilferage and claims arising from such incidents. $14 million has been made available for ESS systems in fiscal year 2005 and plans are being developed to either install ESS where none existed before or make use of or supplement existing airport systems to leverage available resources. TSA is working in partnership with airports to find the most cost effective means to install and maintain current and future ESS systems.

Searching checked baggage in view of the passenger obviously mitigates incidents of pilferage, but as inspection stations move away from lobbies and into airport baggage handling areas, ESS will rise in importance as will emphasis on proper supervision of such areas.

Recommendation 2.—Include a module on professional ethics in its screening training curriculum.

A general ethics course is under development and should be available on the Online Learning Center in the next 4–6 weeks. This course will be mandatory for all TSA employees, with a second component required for all supervisors available during the same timeframe. New employees will have 90 days to complete this course. For existing employees, the training will be required within 6 months.

On pages six and seven of the draft report, there is discussion of previous cases of prosecution against TSA screeners based on "sting" or surveillance evidence. The Office of Workforce Performance and Training will incorporate the occurrence of such incidents into an existing lesson that is currently taught in all three of the basic screener training courses (Dual Function Screener, Passenger, and Baggage).

Currently, TSA screeners do receive some ethics training though they are not required to receive annual ethics training because they do not file financial disclosure reports. The field attorneys at the Office of Chief Counsel often make annual ethics training sessions for financial disclosure filers at their airports available to the screener workforce as well. TSA screeners received the TSA Guide to Major Ethics Rules as new employees. Also, all employees must sign the TSA HRM Letter No. 735–1, Interim Policy on Employee Responsibilities and Conduct, which contains many of the Standards of Ethical Conduct provisions. Field attorneys have also displayed ethics posters in TSA offices and breakrooms.

Additionally, in 2003 and 2004, several articles in The Sentinel were published on ethics issues, including the 14 Principles of Ethical Conduct, gifts, buddy passes,

and the Hatch Act. The Sentinel is a newsletter distributed to the entire TSA workforce.

Recommendation 3.—Resume negotiating an agreement with the airline industry on shared liability for lost or stolen baggage claims.

TSA recently resumed discussions with the airline industry based on the following set of objectives: (1) improve customer service, including communication to the passengers about where to file claims; (2) enhance detection of fraud, including duplicative claims; (3) facilitate cooperation in resolving exceptional claims when necessary; and (4) develop open channels of communication between the Claims Management Office and airline claims offices.

At a meeting on January 11, 2005, the airlines were receptive to these proposed goals, and TSA provided a white paper to the airline community describing our proposed goals in June 2005. The airline associations will then share this paper with their members and provide feedback to TSA. The goal is to have a memorandum of cooperation that all domestic airlines are able to sign by late summer 2005.

General Comment to the Report.—The topic of property inadvertently left out of bags is discussed on page 7 of the OIG report. TSA recognizes that this is a problem and has advised that this property be handled as lost and unclaimed property. Under lost and unclaimed procedures, property recovered after checked baggage has been screened will be inventoried and held for at least 30 days to provide the owner an opportunity to reclaim the property. Should it be unfeasible or impractical for the owner to reclaim the property in a timely fashion, and he or she has evidence that TSA opened his or her baggage through such means as a Notice of Inspection, the passenger may submit a claim for the missing property.

Question. How do you track a screener's progress in terms of consistently utilizing the skills and delivering the appropriate and acceptable service and security they've been trained to deliver?

Answer. As mandated in a February 2004 TSA Management Directive, all training accomplishments must be documented in TSA's centralized Online Learning Center (OLC). TSA management routinely monitors compliance with mandatory training requirements and recurrent training guidelines. Federal Security Directors (FSD) are responsible for ensuring compliance locally on an individual basis.

The aforementioned management directive has been updated as part of the routine annual review cycle and was circulated for comment within TSA in May 2005. This update includes clear language on the responsibility of the training administrator to document all required training within 30 days (7 days for screener basic training), the supervisor's responsibility to ensure their employees have completed all required training, and the role of the course sponsor to monitor national compliance with program requirements. TSA intends to ensure that all employees complete the required amount of training by incorporating this requirement into the fiscal year 2006 Performance Agreements of all TSA supervisors.

In May 2005, the OLC was enhanced to include a much more robust reporting engine that will provide Training Administrators and Course Sponsors with detailed accountability reports.

Additionally, screeners must undergo re-certification each year. The re-certification program for 2004–2005 includes three separate paths: passenger, dual function, and baggage. Passenger screeners must pass three modules. Module 1 is a job knowledge, Standard Operating Procedures (SOP)-specific test. Module 2 is an image test. Module 3 contains practical skills demonstrations. Dual function screeners take both job knowledge tests for passenger and baggage screeners, an image test, and practical skills demonstrations. Baggage screeners must pass two modules, a job knowledge, SOP-specific test and practical skills demonstrations.

To be re-certified, screeners have to pass all applicable modules of the Knowledge and Skills Assessment Program and achieve a rating of meets or exceeds' standards on their annual Personal Performance Assessment. Screeners are afforded one opportunity for remediation and retest. Following a retest, those screeners who fail to re-certify are terminated.

Question. How do you hold the screeners accountable for inappropriate behavior?

Answer. The responsibility and accountability for employee conduct issues rests with the Federal Security Directors at airports. TSA has implemented a leadership model that requires managers to address behaviors that fail to support the TSA mission and to work with employees to engage in appropriate behaviors or face consequences for continued patterns of misconduct. TSA has also implemented policies to implement single step termination procedures for high-risk offenses such as illegal drug use, alcohol on duty, and theft. TSA regards the commission of such offenses as posing a potential security risk. TSA is always mindful of ensuring that due process protections for employees are maintained and has appropriate appeal mechanisms for conduct matters to include the Disciplinary Review Board, the

Agency Grievance process and appeals to the Office of Civil Rights. In addition, TSA has a Professional Review Board at headquarters to review and take appropriate action for misconduct involving senior level employees.

Question. What are the penalties for poor performance?

Answer. The penalties for poor performance range from counseling to removal depending upon the nature, cause, and severity of the performance deficiency. Additionally, screeners must undergo re-certification each year. Failure to re-certify may result in termination or, in special cases, retraining.

Question. In the worst case what is the threshold for removal from work?

Answer. TSA has established mandatory termination procedures for offenses such as illegal drug use, alcohol on duty, and theft. TSA regards the commission of such offenses as posing a potential security risk. In addition, TSA has established policies for first offense terminations for matters affecting integrity and security at the airport such as sleeping on duty, violations of Standard Operating Procedures, security breaches, and criminal conduct.

Question. With such a high workmen's compensation number—one of the highest of the Federal workforce—is there specialized training in place to address this?

Answer. In early fiscal year 2003, TSA met Congressional deadlines to hire Federal airport passenger screeners and achieve checked baggage screening using Explosive Detection Systems. As the TSA screening workforce was deployed, it became apparent that injuries caused by lifting and quickly moving baggage were a serious problem. TSA initiated a safety program in the second quarter of fiscal year 2003 to address the high rate of injuries.

Fiscal year 2004's rate increase from fiscal year 2003 is attributed, in part, to the processing of backlogged claims from incidents that actually occurred in fiscal year 2003. In fiscal year 2004, TSA began implementation of an Occupational Safety and Health program aimed at lowering TSA's injury and illness rate. By the midpoint of fiscal year 2004, a decrease in the number of claims could be seen, and the decrease appears to be continuing into fiscal year 2005. Training, guidance, a nurse intervention program, and the availability of field safety support have contributed significantly to the decrease. For example, in the first 15 weeks of operation, the nurse intervention program at 21 pilot airports yielded savings of over $2.2 million.

It is important to emphasize that airline baggage handling is among the most injury prone occupations in the private sector. TSA is committed to the well-being of its employees and is taking the steps necessary to reduce screener injuries by improving working conditions and appropriately managing the claims process.

TSA has also distributed a safety awareness Web-Based Training (WBT) course both as a CD and via the Online Learning Center. This safety awareness WBT course covers such topics as proper lifting techniques, heat injury prevention, and checkpoint and checked baggage safety. In addition, training on radiation safety awareness is being developed.

TSA "NO FLY" LISTS/SECURE FLIGHT

Question. How does one get on the "no fly list", and more importantly, how does someone get off the list?

Answer. U.S. Government intelligence and law enforcement agencies collect, analyze, and evaluate data used to nominate subjects to the No-Fly List. Intelligence analysts and law enforcement officers within these organizations carefully review nominations based on the No-Fly List criteria and thoroughly evaluate the information during each step of the process. Watch List nominations often contain classified and/or sensitive law enforcement investigative information. Nominations that meet the established criteria are forwarded to the National Counterterrorism Center (NCTC) and the Terrorist Screening Center for inclusion in the TSC Data Base (TSDB) and for addition to the No-Fly List. Time sensitive nominations may be routed directly to the TSC if required.

If it is determined that a person on the No-Fly List should no longer be identified as a No-Fly subject, they will be removed from the list. If additional intelligence data is developed or a subject has been interviewed by U.S. Government officials and deemed no longer a threat, an official request for removal must be submitted to the agency that placed the individual on the list. The original nominating agency will evaluate the data and determine whether the person stays on or is removed from the No-Fly List. The nominating agency will then make a formal request through the nomination chain requesting that the person be removed from the No-Fly List. In some cases, a review of the derogatory information associated with a No-Fly nomination may result in the subject being downgraded to the TSA Selectee List.

The TSA Office of Transportation Security Redress is currently developing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have been erroneously placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information. The redress process will be coordinated with other DHS redress processes as appropriate.

TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

Question. What is TSA doing to address the fact that people are erroneously placed on the list or have mistaken identities?

Answer. TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

The TSA Office of Transportation Security Redress is currently developing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have erroneously been placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information.

Question. What's the appeal process for these people? Is it within or outside TSA?

Answer. TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that

these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

Question. Is there legal recourse for those mistakenly put on the list?

Answer. The TSA Office of Transportation Security Redress is currently developing a redress process for addressing any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have erroneously been placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information.

Question. What is the Department doing to address the serious concerns about privacy and the use of personal passenger information?

Answer. To protect passengers' personal information and civil liberties, TSA and the Secure Flight program will:

—Limit the collection of personal information to only what conforms to the relevant and necessary standard according to The Privacy Act of 1974 (5 U.S.C. 552 (a));

—Limit access to the information to only those TSA employees and contractors who have a "need to know" clearance in order to perform their duties associated with Secure Flight operations;

—Ensure that each employee and contractor associated with the Secure Flight program has completed the TSA mandatory privacy training prior to beginning work on the program;

—Limit sharing of personal information to the Federal Bureau of Investigation (FBI) and intelligence agencies that need the information for investigatory purposes related to aviation security, in accordance with TSA's Privacy Act System of Records Notice published for the program;

—Include a built-in auditing mechanism to detect unauthorized access to the personal information stored for the program;

—Limit the retention of the data. TSA has requested that the National Archives and Records Administration approve a 72-hour retention period for the information collected and used for the Secure Flight program unless a longer retention period is requested by the passenger for redress; and

—Include robust redress mechanisms to enable passengers to work with TSA to resolve instances in which they think they are being inappropriately selected for secondary screening or they are having a difficult time obtaining boarding passes.

Question. TSA has a program under development, called Secure Flight which takes personal passenger information and compares it to the "no fly list" in an effort to identify suspected terrorists traveling by air. How do you respond to concerns raised by both the DHS OIG and the GAO about the Department's handling and use of the personal passenger information related to Secure Flight? What are you doing to remedy the situation?

Answer. To protect passengers' personal information and civil liberties, TSA and the Secure Flight program will:

—Limit the collection of personal information to only what conforms to the relevant and necessary standard according to The Privacy Act of 1974 (5 U.S.C. 552 (a));

—Limit access to the information to only those TSA employees and contractors who have a "need to know" clearance in order to perform their duties associated with Secure Flight operations;

—Ensure that each employee and contractor associated with the Secure Flight program has completed the TSA mandatory privacy training prior to beginning work on the program;

—Limit sharing of personal information to the FBI and intelligence agencies that need the information for investigatory purposes related to aviation security, in accordance with TSA's Privacy Act System of Records Notice published for the program;

—Include a built-in auditing mechanism to detect unauthorized access to the personal information stored for the program;

—Limit the retention of the data. TSA has requested that the National Archives and Records Administration approve a 72-hour retention period for the information collected and used for the Secure Flight program unless a longer retention period is requested by the passenger for redress; and

—Include robust redress mechanisms to enable passengers to work with TSA to resolve instances in which they think they are being inappropriately selected for

secondary screening or they are having a difficult time obtaining boarding passes.

Question. Why did you discontinue development of Secure Flight's predecessor CAPPS II?

Answer. On September 24, 2004, DHS announced its intent to implement a next generation aviation passenger pre-screening program called Secure Flight. Unlike CAPPS II, Secure Flight will focus only on identifying potential terrorist threats (those people on watch lists) and, if a decision is made to use commercial data, it will be utilized in a focused and limited manner. Under Secure Flight, TSA will take over from the air carriers responsibility for the comparison of domestic airline Passenger Name Record (PNR) information against terrorist watch lists. Secure Flight will meet DHS' goals of improving the security and safety of travelers on domestic flights, reducing passenger airport screening time, and protecting privacy and civil liberties. Consistent with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), TSA will begin implementing Secure Flight in August 2005.

TSA recently concluded initial system effectiveness testing for Secure Flight. The commercial data testing began on March 18, 2005, and preliminary test results for the commercial data testing are expected later in 2005.

Secure Flight is designed to improve the efficiency of the prescreening process and reduce the number of people selected for secondary screening. TSA will compare domestic flight PNR information against records contained in the consolidated watch lists contained in the Terrorist Screening Data Base (TSDB), including the expanded No Fly and Selectee lists. Consolidating these checks within the Federal Government will allow TSA to automate most watch list comparisons and apply more consistent, internal analytical procedures when automated resolution of initial "hits" is not possible. Secure Flight will help eliminate false positive watch list matches, improve passengers' experience under the existing system by helping move passengers through airport screening more quickly, reduce the number of individuals selected for secondary screening, and allow for more consistent response procedures at airports for those passengers identified as potential matches. Consequently, TSA will be able to concentrate its screening resources more efficiently.

Finally, Secure Flight will only pre-screen travelers on domestic flights, while CBP will continue to vet passengers on international flights.

AIR TRAVELER SATISFACTION

Question. TSA is one of DHS' most visible agencies since they interact with the air traveling public on a daily basis. What is the most common complaint TSA receives?

Answer. TSA captures complaints reported at airports using TSA's web-based Performance Measurement Information System (PMIS). In April 2005, the most common complaint recorded by TSA's PMIS was the addition of butane lighters to TSA's Prohibited Items List, which was required by IRTPA (Public Law 108–458), Section 4025.

The most common complaint currently received by the TSA Contact Center (TCC) and recorded in the Inquiry Management System (IMS) involves the delays passengers experience during the airport check-in process as a result of having a name similar to, or the same as, individuals who are on a Federal watch list.

Question. Recently, TSA completed a customer satisfaction survey, what did it find?

Answer. The TSA developed the Customer Satisfaction Index for Aviation (CSI–A), which is a performance measure of our aviation screening program. The CSI–A score represents the customer satisfaction response based on a scale of zero to 100 percent where zero represents "very dissatisfied" and 100 percent represents "very satisfied". The CSI–A provides customer service and maintains public confidence while maintaining a high level of security. There are three components of the CSI–A: passenger surveys conducted at airports, national poll results conducted by the Bureau of Transportation Statistics (BTS), and complaints and compliments received by TSA.

The CSI–A score for fiscal year 2005 is 79 percent. The following scores reflect the breakout of each component:

—Passenger surveys conducted at airports=79 percent

—National poll results=75 percent

—Trend of complaints and compliments received by TSA=no significant change in trends

—The change in trends indicate the changes in feedback (complaint and compliments) received by TSA via the Performance Measurement Information Sys-

tem and the TSA Call Center. The aforementioned trend indicated the changes in feedback against time for fiscal year 2004.

Highlights of the 2005 passenger satisfaction survey are as follows:

—91 percent of passengers were satisfied with their overall experience at the passenger checkpoint;

—89 percent of passengers thought security was adequate, as opposed to excessive; and

—82 percent of passengers have confidence in TSA's ability to keep air travel secure.

Question. What other means are you using to validate the customer feedback findings of the survey?

Answer. TSA collects customer feedback on a daily basis. Customers have two means through which to provide feedback on their experience—providing the feedback while at the airport or contacting the TCC. Feedback received at airports is recorded using the web-based system known as the PMIS. PMIS enables TSA personnel at airports to record the feedback received from customers on a daily basis. In addition, PMIS offers airports the ability to record the number of compliments and complaints received according to a variety of categories. The categories are the same as those used by the TCC. Examples of categories include, but are not limited to: discourteous treatment, slow processing, and improper handling of property. This data in addition to the data from the TCC contributes to one of the three components of the Customer Satisfaction Index for Aviation.

Question. What role does the TSA Contact Center play regarding customer service?

Answer. The TCC serves as TSA's central customer service point of contact for all non-media public inquiries. These inquiries can be made to the TCC via telephone, facsimile, correspondence, and e-mail. The inquiries usually take the form of compliments, complaints, or requests for information on a particular issue or problem. For example, an individual may have a question regarding whether a particular item is prohibited in either checked or carry-on luggage and the Customer Service Representative (CSR) or agent will respond accordingly. If an individual has a complaint, the CSR will either attempt to resolve the matter or, if appropriate, refer the matter to a Customer Support and Quality Improvement Manager at the airport for appropriate action and follow-up with that individual. In addition, given the nature of the contact, a matter may need to be elevated to TCC management and/or referred to a program office within TSA for assistance. Furthermore, based on investigation or analysis of complaints and inquiries made to the TCC, recommendations are made to improve agency policies, procedures and practices.

The TCC also performs a security role in protecting the Nation's transportation systems. For example, the TCC forwards to TSA's Transportation Security Operations Center (TSOC) any communications or contacts mentioning, referencing, or alleging threats or security vulnerabilities. The TSOC will then take appropriate action to resolve the issue.

Question. What progress and improvements has TSA made using both the survey and the Center's feedback?

Answer. All feedback received by the passengers is used to make management decisions. Trend analyses, such as review of the top three complaints, are provided and reviewed by senior leadership on a monthly basis. Specific issues that are the result of recent policy changes are also addressed, such as recent complaints on pat-down searches and the amended Prohibited Items List. TSA headquarters is also rolling out a pilot program at ten airports to test a standardized customer comment card. The card is designed to provide a means for convenient and quick feedback at the airport level.

Question. How do you respond to the recent Government Security News article that passengers prefer private screeners' treatment of the passengers being screened?

Answer. The TSA annual customer service survey showed that for the second year in a row there was very little difference in the high degree of confidence and satisfaction air travelers have in TSA-trained screeners—Federal or private. For the second year in a row, air travelers gave consistently high marks to TSA's security screeners. Between 80 and 95 percent of passengers gave positive responses when asked about seven aspects of the Federal security screening process, which included thoroughness and courtesy of screeners as well as confidence in TSA's ability to keep air travel secure. In addition, on average TSA is meeting or exceeding passenger expectations for security line wait times.

Question. How are your wait times and your wait time web page working for TSA?

Answer. TSA continually seeks to evaluate and understand factors that increase wait times and how our service and staffing models can decrease wait times and

improve the screening process for passengers. All airports collect and report wait time data each hour of each day and on the half hour during peak hours of the day. This allows TSA to monitor the customer experience in order to ensure the traveling public is not overburdened with lengthy wait times while not compromising security. The wait time data is used to make improvements to checkpoint configurations and appropriate staffing levels.

Since collection of wait time data, the national average wait time has decreased to less than three minutes. Similarly, the average wait time during peak periods has decreased by almost four minutes since January 2004.

Month	Nationwide average wait time	Nationwide average peak wait time
January 2004	3.35 minutes	14.0 minutes
April 2005	2.95 minutes	10.1 minutes

In addition to using wait time internally to assist in identifying areas for improvement, TSA posts the wait time data on a public internet site available to travelers and the media. The URL can be found at http://waittime.tsa.dhs.gov/index.html. The web site provides the traveling public rolling average wait time by hour, by airport checkpoint, and by day of the week.

Question. What recourse do complainants have?

Answer. The recourse for complainants varies depending on the nature of the complaint. In the majority of cases, the matter is resolved by the Customer Service Representative (CSR) or agent who initially handles the inquiry by providing the individual with information as to why a particular action was taken or about processes currently in place. For example, in some cases, a TSA representative explains the redress process, usually used with claims or watch list issues, and provides the necessary forms. Unusual or less common complaints may need to be elevated to management and/or referred to the appropriate program office. This process ensures that TSA responds in a timely manner to inquiries received, while at the same time giving proper attention to any new trends or issues concerning TSA services. When an issue involves a particular airport, TSA refers the issue to a Customer Support and Quality Improvement Manager at the airport for appropriate action and follow-up with the complainant. The TSA Contact Center (TCC) is another vital tool and serves as TSA's central customer service point of contact for all non-media public inquiries. TSA headquarters is rolling out a pilot program at ten airports to test a standardized customer comment card. The card is designed to provide a means for convenient and quick feedback at the airport level. Additionally, TSA leadership contact information is on the website for program-related issues.

Question. How many complaints does TSA receive and what's the average time for complaints to be resolved?

Answer. At present, there is no single mechanism that captures all customer complaints, compliments, and inquiries. Currently, the system is not structured in a manner that separately breaks out numbers of compliments, complaints, and requests for information within any given subject matter category.

The TCC handles approximately 40,000 non-media inquiries or contacts from the traveling public, including complaints, on a monthly basis. In addition, TSA receives complaints, as well as other types of contacts, through other channels. For example, the Claims Management Office (CMO) receives approximately 2,400 claims on a monthly basis. Customer comments also come into TSA through Customer Support and Quality Improvement Managers at airports. At this time, there is no system that centrally tracks the complaints received by TSA through its various channels.

The time it takes to resolve any particular complaint varies depending on the nature of the complaint. In the majority of cases, the matter is resolved by the CSR or agent who initially handles the inquiry by providing the individual with information as to why a particular action was taken or about processes currently in place and the average talk time for these calls is approximately four minutes. The TCC does not currently track how long it takes to resolve a matter when an agent needs to elevate a call to a particular program office or the field for resolution.

Question. Is there a customer service function in TSA to take complaints at each airport and if so what types of training do these employees receive?

Answer. Many airports have a staff person assigned to manage the customer service function. The staff position is called Customer Support and Quality Improvement Manager (CSQIM). The CSQIM works closely with TCC to receive and respond to complaints and inquiries at the airport level.

Some airports have forms available for customer comments at the checkpoints. TSA headquarters is rolling out a pilot program at ten airports to test a standardized customer comment card. The card is designed to provide a means for convenient and quick feedback at the airport level.

Customer service courses are offered to CSQIM employees via the TSA online training center. Five customer service courses are now available (see descriptions below). An in-service training program, designed specifically for CSQIM employees, is being researched for future implementation.

Excellence in Service.—Fundamentals for Managers will help you develop the skills needed to effectively relate to customers, fulfill their basic needs, and exceed their expectations. You will be provided with opportunities to differentiate between internal and external customers, take ownership for customers' needs, and make sure your customers are completely satisfied.

In "Excellence in Service.—Working with Upset Customers," you will learn how to successfully serve upset customers, calm upset customers, and deal with abusive customers. In addition, you will learn how to control your own emotions and reduce your level of stress.

In "Excellence in Service.—Communicating with Your Customers," you will learn how to build rapport with your customers, and discover how non-verbal communication is interpreted by customers. In addition, you will learn telephone skills, including how to project professionalism and how to provide quality customer service over the telephone. Finally, you will learn how to communicate effectively with your customers through e-mail.

In "Excellence in Service.—Providing Superior Customer Service," you will learn how to develop and maintain a positive attitude, show extra attentiveness to your customers, and use customer-friendly language. In addition, you will learn how to effectively solve customers' problems and benefit from their complaints.

In "Excellence in Service.—Establishing Service Standards," you will learn what customers really want from your organization and how they evaluate your service, as well as how to create and implement effective service standards. In addition, you will learn how to monitor your service standards and how to correct problems that cause service to fall below the standards.

Question. Do you find that the complaints are related to TSA's security measures and the navigation through the airports or is it related to interactions with the airlines?

Answer. The TCC is responsible for handling all non-media inquiries from the traveling public. Each contact is assigned a subject category based upon the nature of the call. Among the available subject categories, one captures "Airline Issues" and another captures "Airport Issues." Airline issues generally involve matters related to proper identification, gate and boarding passes, baggage match and weight/size allowance, airline employee/service complaints, and refunds (airline tickets, lodging). Airport issues generally involve matters related to airport grounds, parking, checkpoint, configuration and limitations. Other categories capture a variety of TSA-related topics. In March 2005, the TCC handled 2,245 contacts involving airline issues, which represents approximately 5 percent of the total contacts handled. With respect to airport issues, 179 contacts were handled in March 2005, less than 1 percent of the total contacts. In addition to airline issues and airport issues, the TCC handled 9,106 contacts involving the No Fly list during March 2005.

R&D CONSOLIDATION

Question. The fiscal year 2006 budget proposes to consolidate all research and development of the Department of Homeland Security into Science and Technology, with the exception of the Domestic Nuclear Detection Office (DNDO). Mr. Secretary, can you tell us what the driving force is behind this consolidation?

Answer. Through the Homeland Security Act of 2002 and subsequent legislation, the Under Secretary for Science and Technology has been tasked with coordinating and integrating all research, development, demonstration, testing, and evaluation (RDT&E) activities of DHS and also to consolidate all Departmental research and development funding within the science and technology programs. The coordination and integration of RDT&E will: maximize the efficiency and effectiveness of the Department's RDT&E capacity; develop and expand synergistic RDT&E programs that cut across the Department's activities; create a world-class RDT&E capability; allow the other Directorates and organizational elements to eliminate within them the specialized management infrastructure required to manage organic RDT&E; and allow the other Directorates and organizational elements within DHS to focus on their operational missions.

Question. What savings do you hope to realize as a result of the consolidation?

Answer. This consolidation will bring under a single accountable authority the scientific and engineering personnel and other RDT&E resources of the Department. Coordination and integration of RDT&E will contribute to a synergistic environment wherein knowledge, capabilities, and initiatives can be leveraged and effectiveness and efficiencies can be enhanced.

Question. How will the consolidation change the way in which research and development is carried out within the Department today?

Answer. Consolidation will contribute to: maximize the efficiency and effectiveness of the Department's RDT&E capacity; develop and expand synergistic RDT&E programs that cut across the Department's activities; create a world-class RDT&E capability; allow the other Directorates and organizational elements to eliminate within them the specialized management infrastructure required to manage organic RDT&E; and allow the other Directorates and organizational elements within DHS to focus on their operational missions.

Question. What assurances can the Department provide to the Committee that the traditional mission of the Coast Guard will continue to flourish in the new consolidated research and development structure?

Answer. Authorities for the U.S. Coast Guard (USCG) RDT&E will rest within USCG, but the USCG RDT&E program will be coordinated with the overall departmental RDT&E program to maximize efficiency and minimize duplication of effort. There are significant efficiencies to be gained with an integrated RATE effort for the Department under a single accountable authority. The S&T Directorate is committed to and responsible for supporting the research, development, testing, and evaluation requirements to ehnance the USCG homeland and non-homeland security mission performance.

Question. Why isn't the DNDO research and development included in this consolidation, would it not benefit as well?

Answer. The Domestic Nuclear Detection Office (DNDO) serves as a unique entity within the Department to consolidate all nuclear-detection related activities, allowing for the development of an integrated office that will be responsible not only for research and development, but also for developing a global nuclear detection architecture and developing and implementing a domestic detection system, to include acquisition programs for detection assets and operational support functions. This integration, as well as coordination with nuclear detection programs in other departments, will allow for the development of a single, global nuclear detection architecture to protect the Nation from attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

DNDO will continue to closely interface with the S&T Directorate on joint projects, as appropriate, for the development of technologies that may provide countermeasures against multiple threat types. The separation of the DNDO nuclear detection RDT&E from the RDT&E conducted within the S&T Directorate will be conducted so as to not have any detrimental effect on potential collaborative efforts that would be gained through the S&T consolidation effort. The goal is to make sure that this Nation maintains a preeminent research and development program to address the technical challenges in radiation detection science and technology, while at the same time capitalizing on the benefits of integrating this program with larger acquisition and operational support efforts.

DOMESTIC NUCLEAR DETECTION OFFICE

Question. Mr. Secretary, I understand from recent news reports that you established the Domestic Nuclear Detection Office 2 days after your arrival at the Department. Further, I understand this office was operational prior to your reorganization notification pursuant to the Homeland Security Act establishing this office directly under the Office of the Secretary. The Committee has also just received a reprogramming request to provide fiscal year 2005 resources to support this office. Where did you get the initial resources and staff to stand up this office?

Answer. The DNDO is a part of a natural evolution of the DHS S&T Radiological and Nuclear Countermeasures portfolio, which was appropriated $122.6 million in fiscal year 2005. Of this appropriation, $92.5 million was to be used to manage programs that directly fall within the mission space of the DNDO, as currently envisioned. The programs that currently are managed through this appropriation, along with the associated staff, will ultimately fall under the management of DNDO. Additionally, a number of other departments and DHS components have provided staff, on a non-reimbursable basis, to the DNDO transition team, which will eventually form the initial staff for the office.

The defense of this Nation against a terrorist nuclear attack is one of the top priorities of the Department, and the attention that I gave this matter immediately

upon my arrival should be indicative of that. I sent out a memo to the Department on March 16, outlining my intention to establish the DNDO, and directing senior members of the Department to support the transition and establishment of the office. This is a process that is still underway, rather than one that has been concluded. As part of this process, the Committee was notified, on April 13, of a single funding reprogramming to use existing DHS S&T funds, as appropriated, to cover operating costs of the new office for the remainder of fiscal year 2005. Simultaneously, I submitted, in accord with Sec. 872 of the Homeland Security Act of 2002 (Public Law 107–296), notification to Congress of the intent to establish the DNDO within the Department. On April 15, the President issued National Security Presidential Directive-43/Homeland Security Presidential Directive-14, "Domestic Nuclear Detection," directing the establishment of DNDO within the Department.

Question. The Department is required to come before the Committee and receive advance approval for new initiatives, why wasn't the Committee notified in advance of the Office's establishment?

Answer. On April 13, DHS submitted both an 872 notice and an fiscal year 2005 Reprogramming Report to appropriate Authorization and Appropriations Committee members. In anticipation of the notification to Congress, I previously announced to the Department my intent to create the office and established an acting director with authority to begin staffing the office from DHS and the other agencies involved, and to take necessary steps to be functional as soon as possible.

Question. Can you tell the Subcommittee what has changed in the last year to warrant the creation of this office immediately; is it new intelligence, new authorities granted to Homeland, or new vulnerabilities uncovered?

Answer. While there is currently no specific intelligence indicating when or where a nuclear attack might occur, it is expected to take several years to continue to develop and test effective, sustainable countermeasures and deploy and operate systems to interdict an attempted attack by our adversaries. With this in mind, it is important to take steps proactively to strengthen and consolidate efforts to be prepared if and when an attempt should come.

Accordingly, acting now provides the Department with an opportunity to consolidate all nuclear-detection related activities and proceed with a fully integrated approach that will include not only research and development, but also the development of a global nuclear detection architecture and development and implementation of a domestic detection system, including acquisition programs for detection assets and operational support functions. This integration, as well as coordination with nuclear detection programs in other departments, will allow for the development of a single, global nuclear detection architecture to protect the Nation from attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

Question. The Department is taking great pains to consolidate the research and development of the Department under the Science and Technology Directorate. Would you explain the rationale behind why DNDO's research and development should remain separate?

Answer. The DNDO serves as a unique entity within the Department to consolidate all nuclear-detection related activities, allowing for the development of an integrated office that will be responsible not only for research and development, but also for developing a global nuclear detection architecture and developing and implementing a domestic detection system, to include acquisition programs for detection assets and operational support functions. This integration, as well as coordination with nuclear detection programs in other departments, will allow for the development of a single, global nuclear detection architecture to protect the Nation from attempts to import or transport a nuclear device or fissile or radiological material intended for illicit use.

DNDO will continue to closely interface with the S&T Directorate on joint projects, as appropriate, for the development of technologies that may provide countermeasures against multiple threat types. The separation of the DNDO RDT&E from the RDT&E conducted within the S&T Directorate will be conducted so as to not have any detrimental effect on potential collaborative efforts that would be gained through the S&T consolidation effort. The goal is to make sure that this Nation maintains a preeminent research and development program to address the technical challenges in radiation detection science and technology, while at the same time capitalizing on the benefits of integrating this program with larger acquisition and operational support efforts.

ROLE OF SCIENCE AND TECHNOLOGY DIRECTORATE

Question. As you step into the role of Secretary, Mr. Chertoff, how well do you think S&T is carrying out its strategic mission?

Answer. Over these last few months I have closely reviewed the work of the S&T Directorate and believe it is doing very well in carrying out its mission. The most important mission for the S&T Directorate is to develop and deploy cutting-edge technologies and new capabilities so that the dedicated men and women who serve to protect and secure our homeland can perform their jobs more effectively and efficiently. The S&T Directorate uses a risk-based approach to prioritizing and planning, and identifies critical capability gaps before attempting to identify or develop technology solutions. The S&T Directorate then addresses the highest priorities that address the broad threat spectrum as well as supporting the needs of the Department's organizational elements.

Question. During your short tenure, what are the areas of greatest concern to you?

Answer. As I emphasized in my recent 2SR speech, the Department's success in meeting its strategic objectives requires a coordinated risk-based approach to planning and prioritizing its activities, and this approach is being implemented across the Department. Thus, the development and implementation of effective and efficient counter-measures to biological, chemical and explosive threats continues to be an area of emphasis for the Department. Within the Department, the S&T Directorate has the lead in developing effective countermeasures for biological, chemical, radiological/nuclear, and explosives threat agents as well as providing support to the Department's organizational elements. The DNDO has the lead role in radiological/nuclear detection capabilities. Both the S&T Directorate and DNDO are committed to ensuring that the Nation is safer from these threat areas. Additionally, the S&T Directorate remains committed to providing the nation's emergency responders, Border Patrol, Coast Guard, and other members of the responder community with innovative, affordable technologies.

Question. How do we have any confidence that the Department, and S&T specifically, is heading in the right direction? Recent reports indicate that S&T has made little if any progress in actually increasing our security through research and strategic management of our limited research dollars.

Answer. Clearly, the S&T Directorate works to ensure that the nation's Federal, State and local operational end-users have the necessary technological tools to protect and secure our homeland. The S&T Directorate acknowledges and accepts that technology research and development is not a 6 month process but rather a long-term investment of 18 months to 4 years for the technology to mature. The Directorate tends to aim further down the road to ensure that the research and development being conducted today is capable of dealing with emerging threats in the future. All of the S&T Directorate's programs began at the same time, March 2003 or soon thereafter, therefore the S&T Directorate has not yet reached full maturity in many of its critical ongoing efforts.

The S&T Directorate also recognizes the need for technology solutions in the near term. The S&T Directorate's efforts to date have resulted in numerous products that are increasing our security. Included in these are:

—BioWatch, a biological agent detection system, which protects the nation's major population centers from the threat and ramifications of a bioterrorist attack. BioWatch also provided support during the G8, Democratic National Convention and Republican National Convention;

—Developed and transitioned PROTECT, a chemical detection system, to the Washington Metropolitan Area Transit Authority for use in the Washington subway system. PROTECT was also deployed to Boston and New York for the Democratic and Republican National Conventions and remains in the New York subway system;

—Delivered the Threat Vulnerability Integration System (TVIS) and the Threat-Vulnerability Mapper (TVM), to the Information Analysis and Infrastructure Protection (IAIP) Directorate;

—Developed the BTS Technology Vision which include Border Watch, Transportation Watch and Border Net which significantly improves our ability to provide the information necessary to secure our borders;

—Selected four urban areas for the pilot of the Regional Technology Integration (RTI) Initiative;

—Developed a joint port and coastal surveillance prototype designated HAWK-EYE with the United States Coast Guard; and

—Developed a Critical Infrastructure Protection (CIP) Decision Support System (DSS) focused on prioritizing investment, protection, mitigation, response, and recovery strategies related to Critical Infrastructure Protection.

Question. How is S&T assisting in the protection of our critical infrastructure and what relation does that have to the Department's efforts of the Information Analysis and Infrastructure Protection office?

Answer. The S&T Directorate supports the Information Analysis and Infrastructure Protection (IAIP) Directorate in the technical aspects of assessing threats to the nation's critical infrastructure. Through RDT&E, the S&T Directorate is providing specialized technical tools for intelligence analysis and knowledge synthesis. Analytical tools include software algorithms for data extraction, pattern discovery, semantic graph representation, visualization, and modeling and simulation. To support these tools, the S&T Directorate also provides tools to the IAIP Directorate, such as the Threat Vulnerability Integration System.

Terrorist capability assessments, which are being performed by the national laboratories, also provide expert scientific data and background information analyses to the IAIP Directorate. The specially developed tools greatly extend the capabilities of the commercially available analytical products that are used by the IAIP Directorate. They are designed to work on massive, multimodal, and distributed data sets and to provide real-time, higher accuracy visualization and modeling capabilities.

The S&T Directorate is also developing scientifically based, rational approaches for prioritizing critical infrastructure protection strategies, protection requirements, and resource allocations using modeling, simulation, and analyses to assess vulnerabilities, consequences, and risks; developing and evaluating protection, mitigation, response, and recovery strategies and technologies; and providing real-time support to decision makers during crises and emergencies.

There are several significant examples of this partnership.

For example, the S&T Directorate provides assistance to IAIP in evaluating the scientific and technical capabilities of terrorist groups and organizations to develop and deploy all WMD agents. This is an excellent example of a reciprocal supporting relationship, in that the IAIP Directorate needs S&T Directorate insight into technical issues, while the S&T Directorate needs IAIP Directorate insight into emerging threats. This "swap" of insight allows the S&T Directorate to meet its responsibility for the coordination of RDT&E needed to address those emergent threats.

In addition, countermeasures for WMD (such as chemical, biological, radiological and nuclear threats) are addressed within the S&T Directorate—however this work supports and is developed in coordination with all of the operational elements of DHS including the IAIP Directorate.

Furthermore, the S&T Directorate is developing the Critical Infrastructure Protection Decision Support System (CIP–DSS) in collaboration with several units of the IAIP Directorate and working with the IAIP Directorate's National Infrastructure Simulation and Analysis Center (NISAC) to validate and mature the model.

The S&T Directorate has also developed the annual National Critical Infrastructure Protection (NCIP) R&D Plan in close coordination with the IAIP Directorate. The National Infrastructure Protection Plan (NIPP), developed by the IAIP Directorate, and the NCIP R&D Plan are complementary documents, mutually supportive and coordinated.

Finally, the S&T Directorate, in coordination the IAIP Directorate, is leading RDT&E efforts that will improve the security of the existing cyber infrastructure and provide a foundation for a more secure infrastructure. To protect these infrastructures, we must improve the security of the protocols that underlie Internet communications. Technological advances are necessary to protect against, detect, and respond to attacks on the nation's information infrastructure.

The S&T Directorate has a number of cooperative programs with the IAIP Directorate linking cyber security research to critical infrastructure protection:

—*Process Control System Forum (PCSF).*—This forum was established to accelerate the development of technology that will enhance the security, safety and reliability of process control system (PCS) and supervisory control and data acquisition (SCADA) systems.

—*Control System Security Test Center (CSSTC).*—In collaboration with the Department of Energy and its resources and testing facilities, this program focuses on developing procedures for enumerating the vulnerability of process control systems to cyber attack and finding solutions to correct these weaknesses.

—*Small Business Innovative Research (SBIR) Awards.*—In fiscal year 2004, 13 Phase I SBIR projects were awarded in the area of process control system security. In fiscal year 2005, Phase II SBIRs were awarded to a subset of the Phase I performers, on the following topics: Advanced Security for SCADA Systems, Protection of SCADA Systems Using Physics Based Authentication and Location

Awareness, Improved Security Information Management for SCADA Systems, A Robust Secure Management System for SCADA/EMS Operations, and A Toolkit for Next Generation Electric Power SCADA Security Protection and Research.

The Science and Technology Requirements Council is one process by which the IAIP Directorate and the other component units in DHS convey their RDT&E requirements to the S&T Directorate. Representatives from the IAIP Directorate also are members of the S&T Directorate's Integrated Product Teams, a key mechanism for coordination and planning of DHS RDT&E efforts.

Question. What is on the horizon in terms of the newest threats and related countermeasures under development?

Answer. The Department is working in close collaboration with the DOD, the FBI, members of the Intelligence Community and others to identify potential new threats, assess the nations vulnerabilities to these potential new threats, and the consequences if these potential new threats were successfully used against us. The S&T has the responsibility within the Department to incorporate the risk of these potential new threats into our overall RDT&E process and the development of appropriate countermeasures. Although details can not be provided herein, the S&T Directorate is addressing, for example, potential threats from genetically modified biological organisms and certain types of non-traditional chemical warfare agents to develop appropriate countermeasures.

Question. Can you tell us how S&T has had a direct role in improving the security of the country?

Answer. The nation's advantage in science and technology is a key element in securing the homeland. The most important mission for the S&T Directorate is to develop and deploy cutting-edge technologies and new capabilities so that the dedicated men and women who serve to protect and secure our homeland can perform their jobs more effectively and efficiently. However, the threats to our homeland remain diverse and daunting. The S&T Directorate constantly monitors current and emerging threats and assesses our vulnerabilities to them, develops new and improved capabilities to counter them and mitigate the effects of terrorist attacks should they occur. The S&T Directorate also enhances the conventional missions of the Department to protect and provide assistance to civilians in response to natural disasters, law enforcement needs, and other activities such as maritime search and rescue. Basically the S&T Directorate assists in making DHS operations science-based, intelligence-informed and technology-enabled.

Question. Mr. Secretary, in the President's fiscal year 2006 request is $110 million for the counter man-portable air defense systems, or Counter MANPADS. Can you give us an update on the status of this program?

Answer. DHS is still on schedule to complete Phase II of the Counter MANPADS program and to provide its report to Congress and the Administration at the end of January 2006. This report will include a Concept of Operations, a maintenance approach, data on system effectiveness and reliability, options on how the system may be deployed, restrictions or regulatory changes required to comply with International Traffic in Arms Regulation (ITAR), and Life Cycle and Total Ownership cost estimates. BAE Systems and Northrop Grumman are scheduled to complete their system designs, including Critical Design Reviews in early summer of 2005. Following the review, the contractors will fabricate, install, and test their prototypes on commercial aircraft (late summer and fall of 2005).

By the end of January 2006, each contractor will have delivered two complete units and demonstrated system performance, including the results of studies emphasizing the operational suitability and cost of its systems. They also will have integrated their equipment onto aircraft, and obtained FAA Supplemental Type Certifications for aircraft airworthiness with the countermeasure system installed.

In addition, the requested $110 million provides for a Phase III program to improve operational, affordability, and maintainability issues. Based on interaction with airline stakeholders, an objective was established for system reliability that fits within the commercial airline heavy maintenance or major overhaul schedule of approximately 3,000 flight hours (depending on commercial airplane types).

A primary objective of the Phase III effort is to increase the reliability of the current countermeasure equipment by fielding a number of operational units and conducting laboratory reliability growth testing. DHS S&T estimates that the Phase III efforts will double current countermeasure equipment reliability to achieve the 3,000 hour threshold across airplane types. Additionally, operational and maintenance concepts have been developed, including reducing the requirements of Minimal Equipment List (MEL) and commercial supply chain management practices, that will be evaluated during Phase III. Based on the results of Phase III operational fielding, reliability testing, and evaluation of operational and maintenance procedures, system design alterations will be developed with ITAR considerations in

mind that will make fleet-wide fielding much more affordable and commercially viable.

Question. Are there areas within S&T where the strategic placement of dollars would be most efficiently used?

Answer. The S&T Directorate uses a risked-based approach to prioritizing and planning and identifies critical capability gaps before attempting to identify or develop technology solutions. The S&T Directorate then addresses the highest priorities across the broad threat spectrum as well as supporting the needs of the Department's organizational elements. The Directorate's R&D activities reflect the prioritization of efforts among the many possible threat agents and targets as well as technology development for supporting the organizational elements of the Department and the emergency responder community.

S&T UNIVERSITY PARTNERSHIP PROGRAM

Question. How does the University partnership effort improve DHS' ability to carry out its mission?

Answer. The Homeland Security Act of 2002, as amended, looks to the university community to stimulate, coordinate, leverage and utilize its unique intellectual capital to address current and future homeland security challenges. To maximize the benefits of engaging the multi-disciplinary research capacity of universities and to access current and future generations of researchers and practitioners, a number of focused activities have been established. These include multi-institutional Centers of Excellence built around mission-critical homeland security areas; cooperative research activities with other Federal agencies with homeland security responsibilities; support of undergraduate, graduate and postdoctoral students to develop a cadre of talent committed to homeland security programs; and outreach to the broader education community. These activities will help ensure that DHS will have the scientific knowledge and talent to successfully address homeland security challenges.

Question. Mr. Secretary, what unique role does S&T play with regard to university research and why is it important?

Answer. The S&T Directorate continues to identify knowledge and capability gap areas that need to be addressed to deal with current and future homeland security threats and the development of countermeasures to those threats. Many of these areas are well suited to university research, development and educational capabilities. Universities provide state-of-the-art research experts experienced and successful in cross- disciplinary programs, access to national and local talent pools and a neutral setting to consider important policy issues. These capabilities and ensuing cross fertilization directly benefit the operational responsibilities of the S&T Directorate.

Question. Are these projects that receive funding chosen by peer review and what does the Department gain by having funded a specific project?

Answer. All projects funded within University Programs are the result of a rigorous and competitive peer and relevancy review process. This includes all research and educational programs. With regard to the Centers of Excellence, in selecting research areas, the S&T Directorate seeks input from a variety of sources. These sources include the Homeland Security Act of 2002, as amended; the National Research Council (NRC); the Homeland Security Presidential Directives (HSPDs); other DHS directorates; and subject matter experts. DHS personnel interact extensively with the funded Centers of Excellence by serving on their review committees, attending workshops and exploring joint research initiatives. In this manner, DHS stays aware of their mission-critical research.

Question. Mr. Secretary, contained in the President's fiscal year 2006 budget request is $22.9 million for the National Bio and Agrodefense Facility. What is the mission of this facility and why isn't it in the Center for Disease Control's or U.S. Department of Agriculture's budget request?

Answer. HSPD–9 ("Defense of United States Agriculture and Food", paragraph 24) states: "The Secretaries of Agriculture and Homeland Security will develop a plan to provide safe, secure, and state-of-the-art agriculture bio-containment laboratories that research and develop diagnostic capabilities for foreign animal and zoonotic diseases." The S&T Directorate currently has responsibility for one such facility, as the Homeland Security Act of 2002 transferred the "assets and liabilities" of the Plum Island Animal Disease Center (PIADC) from USDA to DHS as of March 1, 2003. PIADC is currently the nation's only Bio-Safety Level 3 facility (BSL–3Ag) for research and diagnostic programs on foreign animal diseases such as foot-and-mouth disease (FMD). The bio-containment laboratories and animal facilities at PIADC are aged well beyond their originally designed life expectancy, and are in

immediate need of re-capitalization or replacement. There is no BSL–4 livestock capable laboratory at PIADC or elsewhere in the United States to work on high consequence zoonotic diseases in host livestock species. Therefore, planning for the National Biological and Agriculture Facility is the top S&T Directorate priority for biocontainment facilities, and impacts ongoing and planned programs for biological countermeasures for foreign animal diseases (including assays and diagnostics, vaccines and therapeutics, and forensics).

Recognizing the needs described above, the President requested $23 million in fiscal year 2006 for the design and initiation of a National Bio and Agro-defense Facility (NBAF). In preparation for this, we have undertaken a conceptual design study to better characterize the key programmatic requirements driving the NBAF design and to explore the cost benefit tradeoffs associated with each of these drivers. This conceptual design will explore three major NBAF options of increasing capability:

—Keeps the scope the same as the current PIADC mission but builds the facilities required to meet the needs of the first half of the 21st century;

—Expands the scope to include additional agriculture biocontainment laboratories for foreign animal and zoonotic diseases as called for in HSPD–9 above; and

—Adds expanded test and evaluation facilities to support clinical testing of medical countermeasures by the Department of Health and Human Services (HHS).

—DHS is committed to working with Congress, stakeholders, and partner Federal Departments and agencies (e.g. USDA and HHS) in the development of this new facility.

DHS INTELLIGENCE MISSION

Question. Mr. Secretary, your written testimony states that you will work closely with the intelligence community and the Director for National Intelligence. Given that, what is Information Analysis and Infrastructure Protection (IAIP) Directorate's role in the intelligence world since the enactment of the Intelligence Reform Act?

Answer. This role is evolving. The Department makes many contributions to the Intelligence Community and we will continue to enhance those contributions. Systematic intelligence lies at the heart of everything that the Department does. Understanding the enemy's intent and capabilities affects how we operate at our borders, how we assess risk in protecting infrastructure, how we discern the kind of threats for which we must be prepared to respond. We are enhancing our ability to fuse that information and combine it with information from other members of the Intelligence Community, as well as information from our State and local and international partners.

As I announced on July 13, 2005, I have proposed that the Assistant Secretary of Information Analysis become the Chief Intelligence Officer for the Department. My proposal is for the Chief Intelligence Officer to head a strengthened Intelligence and Analysis division that will report directly to me. This office will ensure that intelligence is effectively coordinated, fused and analyzed within the Department so that we have a common operational picture. It will also provide a primary connection between DHS and the Intelligence Community as a whole, and a primary source of information for state, local and private sector partners. The Department's unique access to information from our components, as well as our robust relationship with State, local, and tribal governments, as well as with the private sector, makes our enhanced contribution to the IC critical as we move forward.

In addition, since the creation of the Director of National Intelligence, IAIP, through the Office of Information Analysis, has collaborated with the Office of the Director of National Intelligence (ODNI) on a number of initiatives. IA works closely with the National Counterterrorism Center (NCTC). Among other things, we have provided IA intelligence analyst detailees to the NCTC, who are in a unique position to understand both intelligence information derived from our components and its impact on State and local governments, as well as the private sector. We also work closely with the NCTC to provide data and fuse critical information. We also participate in the WMD Working Group, (an outgrowth of the WMD Commission), the National Framework for Analytical Production working group, which is responsible for developing a national production framework for the IC, and on work dealing with human resource issues. IA will continue to develop a close working relationship with the ODNI as it strives to improve existing programs and put in place new initiatives that will further strengthen and protect our homeland.

Question. Is it the opinion of the Department that IAIP's functions are enhanced or minimized by the Act?

Answer. Greater integration of the Intelligence Community and a heightened emphasis on information sharing as a result of Public Law 108–458, the Intelligence

Reform and Terrorism Prevention Act of 2004 (IRTPA), will strengthen the ability of DHS's Office of Information Analysis to carry out its mission. We are optimistic that these reforms will lead to greater collaboration in analysis and greater ease of exchanging information across all levels. The continued emphasis on information sharing directed by IRTPA, for example, will improve DHS IA's ability to carry out its mission to fuse and lead the Department's intelligence activities and to share and receive critical threat information with and from state, local, territorial, and tribal governments and the private sector.

Question. Can you tell the Subcommittee how the Homeland Security Operations Center's (HSOC) daily activities are changed by the Intelligence Reform Act?

Answer. The daily activities of the HSOC are not changed by the Intelligence Reform Act. The HSOC will continue to provide general domestic situational awareness, a common operational picture, and support to the Interagency Incident Management Group (IIMG) and DHS Leadership, as well as act as the primary conduit for the White House Situation Room and IIMG for domestic situational awareness. HSOC collects domestic related suspicious activity reports throughout the United States and shares that information with DHS stakeholders.

Question. How will the HSOC perform its mission in light of this new Act?

Answer. HSOC will continue to perform its core missions as it has in the past.

Question. How has the Homeland Security Operations Center interfaced with the Terrorist Tracking Information Center which has been absorbed into the National Counterterroism Intelligence Center?

Answer. The HSOC provides general domestic situational awareness, a common operational picture, and support to the IIMG and DHS Leadership, as well as acting as the primary conduit for the White House Situation Room and IIMG for domestic situational awareness. The HSOC will continue to collect domestic related suspicious activity reports, look at domestic terror threats and natural disasters, focusing efforts domestically. HSOC is the lead conduit to State and local agencies. HSOC anticipates being the primary conduit to NCTC for domestic situational awareness.

Question. How will the Homeland Security Operations Center fit into the new intelligence community structure?

Answer. The advent of the new intelligence community structure does not significantly change the daily activities of the HSOC. The HSOC acts as the "ingest" point for threat traffic and suspicious activity reporting to DHS, so it is integral that the information captured and exploited by the Office of Information Analysis (IA) staff in the HSOC is shared with the Federal Intelligence Community. This occurs on a constant basis through video teleconference (0100 Production Meeting hosted by NCTC, the 0800 and 1500 SVTC), telephone, JWICS email and fax. The IA staff in the HSOC works closely with the NCTC Operations Center/FBI Counterterrorism Watch to develop emergent traffic containing a domestic nexus. Additionally, the IA staff in the HSOC is prepared to provide situational awareness to the DNI Operations Center when it is operational.

Question. Do you think the Department should have an Under Secretary of Intelligence to elevate its role within the intelligence community?

Answer. As I announced on July 12, 2005, after conducting 2SR, I believe that the current Assistant Secretary for Information Analysis should become the Chief Intelligence Officer for the Department, and that this component should report directly to me. I am confident that these changes will ensure an enhanced role for the Department's intelligence functions within the Intelligence Community.

CRITICAL INFRASTRUCTURE PROTECTION

Question. The Department recently released an interim report on the Nation's critical infrastructure, the purpose of which is to provide an outline for integrating critical infrastructure protection at the national level. How does this interim report lead to better protection of the Nation's critical infrastructure?

Answer. DHS is coordinating, for the first time, the overall national effort to protect critical infrastructure. The Interim National Infrastructure Protection Plan (NIPP) describes a risk management framework that takes into account threats, vulnerabilities, and consequences to prioritize the nation's critical infrastructure and key resources (CI/KR). The NIPP delineates roles and responsibilities among Federal agencies; state, local, and tribal entities; as well as private sector stakeholders in carrying out infrastructure protection activities within and across the 17 CI/KR sectors established by HSPD–7. The Interim NIPP is intended to foster sector-specific protective strategies and provides a mechanism for coordinating protective actions across sectors. It builds on the nation's existing critical infrastructure protection knowledge base while acknowledging the need to expand dialogue and

partnerships with key public and private sector stakeholders to create an integrated, national critical infrastructure protection program.

Question. My concern is that although the exercise is useful in developing a framework, when it gets down to the details, the momentum is lost and there never seems to be any achievements. How do you intend to use the interim report to translate into actual outcomes?

Answer. The interim NIPP outlines the foundation, processes, and methodologies of the risk management framework. The interim NIPP will be replaced by the final version of the NIPP, which will include sector-specific plans with performance measures.

Question. Did you seek the advice of States, locals and the private sector in the writing of this report?

Answer. Yes, as part of the comment period during July and August of 2004, the preliminary draft NIPP was shared with State and Territorial Homeland Security Advisors and individual members of the private sector for review and comment. The comments from the review were taken into consideration during the development of the Interim NIPP. The period of time dedicated to reviewing the Interim Plan will include additional private sector and stakeholder engagement.

Question. How does this report enable the Department to better identify which infrastructure is critical and what are the criteria for that determination?

Answer. The NIPP risk management framework sets over arching security goals. Once security goals are set, the next step in the framework is to develop and maintain an inventory of the nation's assets. After an asset is identified and basic information on it is collected, DHS employs an initial screening methodology to determine whether or not it is of national consequence. Priority is given to those assets that, if attacked, could have a nationally significant effect.

Question. How do you plan to get this report out to the public? Are you planning on doing town hall meetings, news articles or another forum?

Answer. The success of the national infrastructure protection program, as framed and articulated in the Interim NIPP, is highly dependent on obtaining buy-in and participation from all audiences. DHS is responsible for leading and coordinating the national infrastructure protection program, while the responsibility for carrying out the protective activities is shared among Sector-Specific Agencies, asset owners/operators, and state, local, and tribal governments.

State, local, and tribal entities and private sector stakeholders have an important role to play in protecting the nation's CI/KR. To ensure that assets within these areas are covered within the engagement and outreach process, these stakeholders must be aware of, and participate in, the implementation and the refinement of the Interim NIPP. The initial approach to engage state, local, and tribal entities and private sector stakeholders will be carried out by DHS, in coordination with the Sector Specific Agencies.

Stakeholder outreach and engagement tactics differ greatly by audience and focus on each stakeholder's interests and role in the implementation of a national infrastructure protection program. Accordingly, the Interim NIPP engagement process is organized by audience group, specifically: intra-Federal stakeholders; state, local, and tribal stakeholders; private sector stakeholders; and the media and public.

IAIP HIRING DIFFICULITIES

Question. Of concern to me is the amount of time it takes IAIP to hire and put in place new personnel. These are people who are charged with the intelligence and infrastructure protection functions of the Department. Why is it taking so long, and what can the Subcommittee do to help improve this situation?

Answer. As a result of the competitive market for the cleared community and the unique skills and abilities needed in IAIP, an aggressive recruitment of these talented candidates has been necessary to drive toward our hiring goals. As noted, these candidates are filling important intelligence and infrastructure protection functions. The process of recruiting, selecting, and hiring candidates to meet the Directorate's needs is lengthy because of the multiple steps involved in this process to ensure a complete and thorough evaluation of candidates. However, over the past year IAIP has been successful in implementing improvements to shorten this process.

Working closely with the Office of Personnel Management (OPM), improvements include the development of position descriptions and vacancy announcements that define the minimum requirements for each position. Once the position is posted and an applicant pool is created, a list of qualified candidates is then forwarded by OPM to hiring managers for comprehensive interviews and assessments. Once a selection

has been made, a tentative offer is extended to the candidate contingent upon the successful completion of a security investigation.

IAIP hiring managers take the time necessary in the selection process in order to ensure the specialized needs of the Directorate are met, particularly since many of the vacancies are highly sensitive positions.

Even faced with the competitive market for qualified candidates and the time it takes to on-board candidates, IAIP has been successful in hiring 517 of the 803 FTE allotments to date and will continue to aggressively recruit to meet its hiring target.

The Subcommittee has been very supportive in working with IAIP to understand the implications and expectations required to staff a highly qualified team. The approval to allow direct hiring authority has been instrumental in allowing us to aggressively identify, assess, and hire key staff. The continued active support of the Subcommittee is appreciated as IAIP works to achieve this target hiring goal.

Question. Is the hiring time dependent on another agency to process background checks and clearances?

Answer. Historically, DHS contracted collateral (SECRET and TOP SECRET) as well as TS/SCI security investigations through traditional venues such as Office of Personnel Management and Defense Security Systems (DSS). These venues also provide support to Federal, military and intelligence agencies. Due to high demand, they have continuously experienced severe backlogs, adversely impacting the timely processing of DHS requests.

However, DHS has recently acquired a new venue for security investigations through CBP. CBP now processes TS/SCI clearances for DHS and, due to a smaller workload, has cut down the average time for a security background investigation (with no previous clearance) from 12–18 months to as little as 6–8 weeks. This timeframe is competitive or, in many cases, faster than industry averages within the cleared community.

Under the current projected timeline of the hiring process, the security clearance process accounts for 25 percent of the total hiring process cycle time on average. This is a significant reduction from previous projections (50–60 percent), and is attributed to recent changes in the sourcing of investigations to a new contractor agency.

Question. Is the Department doing anything to help IAIP recruit qualified candidates for such a crucial role?

Answer. DHS has been fully supportive of IAIP recruitment efforts and has included the Directorate in a variety of Department-wide recruitment events to attract qualified candidates. For example, the Department was successful in obtaining direct-hire authority for IAIP's hard to fill positions and the Equal Opportunity Office has partnered with IAIP to attend a Disability Career Fair and Asian Pacific American Federal Career Advancement Summit. IAIP also participated in a DHS-wide career fair at Walter Reed Army Medical Center to recruit disabled veterans in conjunction with the Department of Defense, as well as a DHS-wide Presidential Management Fellows job fair at the Washington Convention Center during the last week in March of this year.

Question. Can you please submit your strategy to the Subcommittee on how you intend to address this problem?

Answer. IAIP is working to implement new ways to improve the candidate selection process to support surge hiring efforts. These include:

—*Posting All Remaining Vacancies.*—Work with hiring managers to expedite the posting of all vacancies on the USAJOBS website;

—*Making Multiple Selections.*—Encourage the practice of making multiple selections from Cert Lists whenever possible;

—*Sharing Cert Lists.*—Facilitate the sharing of Cert Lists are shared among managers with similar hiring needs;

—*Supporting the Recruitment Campaign.*—Encourage managers to attend recruitment events; and

—*Conducting Panel Interviewing.*—Identify Subject Matter Experts to screen qualified candidates for hiring manager review and selection.

Through these efforts, IAIP will institute a systematic process for identifying volume hiring needs, matching those needs with available candidates, and mobilizing hiring managers to make multiple selections in a timely manner. In support of this strategy, IAIP is continuing efforts to broaden the candidate pool through an active recruiting campaign targeting specific hiring needs and an aggressive advertising campaign to publicize opportunities at IAIP.

Question. Is the housing of IAIP personnel still an issue today?

Answer. Yes, housing remains an issue for IAIP, but we are working to overcome them. Among the challenges faced by IAIP is the lack of permanent space. On any given day, there are more than 90 IA employees without a dedicated seat. Staff have

been doubling, tripling, and quadrupling up in seats, working shifts and staggered hours to compensate for the deficit of Sensitive Compartmented Information Facility (SCIF) seating.

To address its facilities situation, IAIP has developed a plan through fiscal year 2006 to place staff in swing and permanent seats on the NAC, and five floors of leased space at an office building in Arlington, VA. The Arlington location is currently partially occupied as swing space while floors are permanently constructed in a planned series. Two floors are nearing completion of permanent construction, with furniture and IT installation to follow. The entire project is scheduled for completion at the end of 2005. The location will eventually have 440 seats, and will house primarily the Office of Infrastructure Protection (IP).

On the NAC, IAIP will occupy part of Building, all of Building 19, and the first and second floors of Building 17. Ultimately, all of Building 19 will be SCIF and will house IA (to include seating for the positions requested in 2006) and the Office of the Under Secretary. Floors one and two of Building 19 are under demolition/power upgrade prior to renovation, which is currently scheduled to be completed in Winter of 2005, with the renovation beginning in the Summer of 2005 and continuing into the Spring of 2006.

IAIP's total SCIF requirement will be met once the Building 19 renovation is completed.

IAIP COORDINATION OF PROTECTION

Question. How does the Department plan to get the necessary support of State and local governments and private sector to protect our critical infrastructure when dollars are tight?

Answer. DHS relies on strong and cooperative relationships with State and local governments and private sector partners to advance overall National protective strategies. The Department understands that local law enforcement, first responders, and the overall readiness and response community have the day-to-day responsibility to protect our citizens and infrastructures. The Federal Government must continue to partner with State and local officials and key leaders in the private sector to ensure available funding is appropriately allocated and correct policies and procedures are in place.

The Department will continue to cultivate and expand its outreach and information sharing components to enhance its relationships with state/local and private sector partners. By continuing to build upon these vital relationships, the Department plans to continually provide the information, policy guidance and risk assessment methodologies necessary to help owners and operators bolster physical and cyber security plans.

Question. How does the Department coordinate with all other efforts by the Federal Government and State and locals, including municipalities to ensure that each entity is putting in place the most effective security measures for a specific piece of infrastructure?

Answer. As part of an ongoing, government-wide effort to protect national infrastructure, DHS is working on several initiatives with other Federal departments, state, local, and tribal governments, and the private sector. These initiatives are designed to protect against known and potential threats; reduce critical infrastructure vulnerabilities in a comprehensive and integrated manner; maximize efficient use of resources for infrastructure protection; build partnerships among Federal, state, local, tribal, private sector, and international stakeholders; and continuously track and improve national infrastructure protection.

In the first of these initiatives, the Department is providing the private sector, law enforcement entities, and State homeland security personnel with technical and material assistance to develop and implement Buffer Zone Protection Plans (BZPPs) around critical infrastructure and key assets. To formulate these plans, owners and operators and local law enforcement work together to identify asset vulnerabilities, gaps in protection, and means of mitigating these vulnerabilities.

The Department is also in the process of deploying all 68 Protective Security Advisors (PSAs) to 60 metropolitan areas throughout the United States. These security specialists serve as DHS representatives permanently assigned in the field. The mission of the PSA is to represent the Office of Infrastructure Protection (IP) in local communities throughout the United States, serving as a liaison between DHS, the private sector, and Federal, state, local, and tribal entities; acting as IP's on-site critical infrastructure and vulnerability assessment specialist; providing expertise and support to the Principal Federal Official(s) responsible for National Special Security Events; and providing real-time information on facility significance and

protective measures. PSAs continue to assist local entities in putting in place the most effective security measures for specific pieces of infrastructure.

DHS is also providing terrorism prevention training to private sector, law enforcement entities, and State homeland security personnel. To date, over 5,600 security personnel have participated in the training courses. Courses relate terrorist threats and tactics to one of several different topics including buffer zone protection plans, soft targets, bombs, underwater hazardous devices, police S.W.A.T. team response, and counter surveillance and emerging threats. This training program provides baseline knowledge for a law enforcement protecting critical infrastructure.

Finally, Government Coordinating Councils (GCCs) are groups being established for each sector that consist of Federal representation involved in the security of all 17 sectors defined by the National Infrastructure Protection Plan (NIPP). The GCCs will serve as a counterpart to industry-sponsored Sector Coordinating Councils (SCC). GCCs, which include a number of agencies with sector infrastructure protection responsibilities, will coordinate with the SCC and work to ensure the implementation of effective sector strategies and initiatives to support the nation's homeland security mission.

Question. What are IAIP and the Department doing about cybersecurity, particularly when it is not governed by any one actor but affects everyone?

Answer. The National Cyber Security Division (NCSD) of IAIP's Office of Infrastructure Protection was created to address cyber security issues and the priorities laid out in the National Strategy to Secure Cyberspace. In addition, HSPD–7 called upon the Department to establish a national focal point for cyber security, which is the mission of NCSD. Both the National Strategy to Secure Cyberspace and HSPD–7 recognize that cyber security is not just one entity's concern or jurisdiction, and both call upon DHS to be a focal point and work with partners in other Federal agencies, academic institutions, the law enforcement and intelligence communities, the private sector, and the general public to improve our cyber security posture.

NCSD's mission, in cooperation with public, private, and international entities, is to secure cyberspace and America's cyber assets. In order to fulfill that mission, NCSD has laid out goals that reflect and guide its priorities and programs, as follow:

—*Goal 1.*—Establish a National Cyber Security Response System to prevent, predict, detect, respond to, and reconstitute rapidly after cyber incidents.

—*Goal 2.*—Work with public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks.

—*Goal 3.*—Promote a comprehensive national awareness program empowering all Americans to secure cyberspace.

—*Goal 4.*—Foster adequate training and education programs to support the nation's cyber security needs.

—*Goal 5.*—Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace.

In addition to the National Strategy to Secure Cyberspace, Homeland Security Presidential Directives, National Security Presidential Directives, the Federal Information Security Management Act (FISMA) provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets; recognizes the highly networked nature of the current Federal computing environment and provides effective government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities; provides for development and maintenance of minimum controls required to protect Federal information and information systems; provides a mechanism for improved oversight of Federal agency information security programs; acknowledges that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the Nation that are designed, built, and operated by the private sector; and recognizes that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products. Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center US–CERT to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

FISMA, Section 3546 states that the Federal information security incident center, US–CERT, will perform the following functions:

—Provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;
—Compile and analyze information about incidents that threaten information security;
—Inform operators of agency information systems about current and potential information security threats and vulnerabilities; and
—Consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters. In accordance with DOD Directive O–8530–1, all DOD services and agencies are to report incidents to the Joint Task Force Global Network Operations (JTF–GNO), which will, in turn, coordinate directly with the US–CERT.

The DHS approach to cybersecurity is one of coordination and collaboration. Therefore, in each of its cybersecurity efforts, DHS works with key stakeholders and subject matter experts, both within the Department and with external constituencies on a Federal, State, local, and international level.

OFFICE OF SECURITY

Question. What is the Department doing to streamline the process of security clearances to prevent a backlog?

Answer. The Department grants access to classified information in a timely manner. There is no adjudicative backlog in the granting of security clearances at the present time.

The Department is continually working to improve the process of conducting and adjudicating background investigations and granting security clearances. DHS is coordinating with other departments and agencies in the personnel security community to accomplish this goal.

Reciprocity.—DHS, like other Executive Branch Departments and agencies, complies with the requirements of Executive Order 12968, which establishes a uniform Federal personnel security program for employees who require access to classified information. The Intelligence Reform and Terrorism Prevention Act and Executive Order 12968 require that background investigations and eligibility determinations should be mutually and reciprocally accepted by Federal agencies. Since its inception, DHS has conformed to this reciprocity requirement.

Interim Secret Security Clearances.—The Department grants interim access to certain classified information following favorable completion of a preliminary investigation. This interim Secret clearance permits DHS employees to begin their service expeditiously. In addition, the Department is working diligently with the Office of Personnel Management to accelerate the investigative process for Top Secret security clearances by obtaining delegations of authority and prioritizing cases.

Certain Investigative Authority.—DHS has obtained certain investigative authority that expedites background investigations and re-investigations for Top Secret and Sensitive Compartmented Information (SCI) security clearances. The Department has utilized the personnel security services of CBP in the Border and Transportation Security Directorate to conduct these background investigations for DHS Headquarters applicants. In this way, DHS has been able to avail itself of process improvements, technological advances, and other management efficiencies.

Additional Adjudicators.—The DHS Office of Security (OS) is hiring additional Federal employees as security clearance adjudicators to meet the Department's growing needs.

Streamlining the Process.—In addition, DHS has taken the following steps to streamline and improve the quality of the security clearance process:

—The Department is focusing its background investigations on the areas most relevant to the current threats facing the country and the Department;
—The Department is applying resources in the early phases of the investigation to maximize limited investigative resources and minimize wasteful expenditure on candidates unlikely to be favorably adjudicated;
—The Department is strategically placing employees to assist other Federal agencies at key points of the investigative process;
—The Department is automating many aspects of the personnel security process, including the deployment of Electronic Questionnaires for Investigations Processing (EQIP), an automated tool that allows applicants to complete the form online, thus reducing the processing time and minimizing the error rate; and

—A team of human capital and personnel security experts are working to increase efficiency by educating managers and prospective employees about the requirements of the security clearance process.

Question. A pending fiscal year 2005 reprogramming request proposes to transfer $6.6 million from the Information Analysis and Infrastructure Protection Directorate to the Office of Security. Will the fiscal year 2006 request of $39.4 million for the Office of Security fully fund the Office of Security so that it does not require transfers from other DHS components to carryout its important operations?

Answer. It is projected that the increase of $39.445 million for fiscal year 2006 will be sufficient for the currently-anticipated requirements of the Office of Security. It should be noted, however, that the proposed House version of the fiscal year 2006 Homeland Security Appropriations Bill cut of $10 million would have a drastic effect on important operations. If this occurs, the Office of Security will again require a transfer of funds from other components or be forced to cut services.

Question. How will the Office of Security assist with the Department's efforts to improve information sharing with State and local governments and private industry?

Answer. The Office of Security (OS) aims to facilitate the sharing process, while ensuring that the dissemination of information is conducted through secure processes and channels to trustworthy individuals. OS continues to play an integral role in the Department's efforts to improve information sharing at all levels through a number of initiatives.

OS has assisted in the following ways:

—*Security Clearances.*—OS has established and implemented processes to facilitate the issuance of security clearances to state, local and private sector personnel, in coordination with the SLGCP and the Infrastructure Coordination Division of the IAIP Directorate.

—*Communications Security.*—OS has developed standards and a process for the deployment of secure communications equipment, in coordination with SLGCP and the DHS Chief Information Officer;

—*Computer Security Standards.*—OS has developed and implemented standards that support the deployment of computer equipment for classified information disseminated to selected State and local government locations;

—*Security Policy Guidance.*—OS has issued policy and procedural guidance to support the sharing of information and encourage secure dissemination to the intended audience; and

—*Security Training.*—OS has prepared and distributed educational and awareness products to designated State and local government personnel and private-sector officials.

OS has played a significant role in the creation of proposed national standards for the sharing and safeguarding of homeland security information.

Question. What coordination will take place between the Office of Security, the Chief Information Officer, and the Information Analysis and Infrastructure Protection Directorate to ensure that sensitive security materials do not fall into the wrong hands?

Answer. The Office of Security (OS) continues to coordinate with the DHS Chief Information Officer (CIO) and the IAIP Directorate to ensure that information shared with state, local and private sector partners is afforded the appropriate protections commensurate with the level of sensitivity.

In addition to the five areas listed in the previous response, OS has: (1) contributed to the development of policies and procedures for the deployment of the HSDN and is an active participant in the Homeland Security Accreditation Working Group, developing guidelines regarding appropriate physical security standards, security clearance verifications, and security training for the HSDN program; (2) provided guidance regarding the "Need to Know" requirements for the network. In addition, OS has contributed to the creation of a Homeland Security Information Network-Secret (HSIN–S) Users Manual to ensure proper security standards for information disseminated through the system; (3) involved in a comprehensive review of information sharing laws, Executive Orders, regulations and guidance, and it has participated in the creation of national standards for the protection of sensitive and classified homeland security information; and (4) participated in weekly meetings with the IAIP Information Sharing and Collaboration Office, a program established to coordinate and facilitate information sharing throughout DHS and with its partners.

REGIONS INITIATIVE

Question. Why has the report required by section 706 of the Homeland Security Act of 2002 not been submitted to Congress?

Answer. The report required by section 706 of the Homeland Security Act of 2002 was submitted in February 2004 as requested.

Question. The fiscal year 2006 budget justification proposes a traveling cadre from the Office of Security that will provide security-related support to regional offices. However, there is no funding identified for this activity. How will the Office of Security provide assistance to these offices without funding?

Answer. The Office of Security is requesting a total of $168,131 for travel in the line item fiscal year 2006 budget. This money will be used by Office of Security personnel to support all travel requirements within the office.

I-STAFF

Question. The Operational Integration Staff and the proposed Office of Policy, Planning, and International Affairs appear to be working toward the same goal of developing cohesiveness among DHS components. How are the roles of the integration staff distinguished from those of the proposed Office of Policy, Planning, and International Affairs?

Answer. The new Office of Policy will lead the Department in both strategic policy development and oversight of all program policy efforts, while consolidating programs with significant policy responsibilities into one cohesive office. The new Office of Operations will provide the Department with a coordinated cross-cutting operation function. The Operation Integration Staff, consequently, will no longer be needed, and most of its current employees will be merged into the Offices of Policy or Operations

Question. The Department has placed the Operational Integration Staff in charge of coordinating the security plans for homeland security events that are not designated National Special Security Events (NSSEs). Please provide an overview of the plan for operational command and control for such events?

Answer. Special Event security is the responsibility of law enforcement agencies with jurisdiction at the event location. The lead agency will normally be the local law enforcement agency. However, a Federal agency may assume the lead role, as with an event at a national park. Generally, because multiple agencies and jurisdictions are involved, a coordinated and integrated approach to event security is involved. As directed by both the Homeland Security Act of 2002 and HSPD–5—"Management of Domestic Incidents," the Department of Homeland Security promulgated the National Incident Management System (NIMS). The NIMS provides a command and control framework within which government and private entities at all levels can work together across each phase of incident management: prevention, preparedness, response, recovery, and mitigation. Specifically, the NIMS requires the formation of a Unified Command to facilitate coordination for incidents and potential incidents involving multiple agencies with independent jurisdictional authority. The Unified Command allows agencies with different legal and functional authorities and responsibilities to work together in an integrated fashion without affecting individual agency authority, responsibility, or accountability. For Special Events below the NSSE threshold, the responsibility for security planning resides entirely within this Unified Command.

The NIMS also recognizes the need for support and coordination for an event and establishes a multi-agency coordination system comprised of local and State Emergency Operations Centers and coordination entities. Under normal circumstances, there is no similar standing Federal coordination entity at the local level, but certain special events below the NSSE threshold create a significant need for Federal interagency coordination. In such cases, the Secretary of Homeland Security appoints a Federal Coordinator to serve as the principal Federal point of coordination. As requests for Federal assistance are answered and as Federal agencies adapt their independent authorities, the Federal Coordinator captures this integrated strategy in the form of a Special Event Integrated Federal Support Plan. The Federal Coordinator then coordinates support and information sharing at the special event and responds to unforeseen support needs and events.

The NIMS protocol does not change the existing command and control architecture at the Unified Command level for agencies supporting the Unified Command, or for agencies forced to adapt their independent operations as a result of an event.

Question. What role (if any) will the Secret Service have in non-NSSE events?

Answer. For non-NSSE events, i.e., DHS-established levels of Special Events Homeland Security (SEHS), the role of the Secret Service will vary dependent upon the circumstances surrounding the particular event. For events that receive a designation of Level I or Level II and have a traditional protectee of the Secret Service in attendance, the Secret Service will implement appropriate protective protocols and may serve as the Federal Coordinator. For events that receive a designation of

Level I or II that do not have a traditional Secret Service protectee in attendance, the Secret Service may offer available protective assets, as appropriate.

When the event receives a lower designation and a protectee will attend, the Secret Service will implement appropriate protective protocols; in those instances when no protectee will attend, the Secret Service may offer protective event management training, as appropriate.

Question. What is the budget for the Operational Integration Staff for fiscal year 2005? Where are those funds coming from?

Answer. As directed by the language in the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief Act, 2005, further funding is not available for the Operational Integration Staff in fiscal year 2005 unless funds are reprogrammed. Travel and incidental costs were borne by the components of those on detail to these efforts.

HUMAN RESOURCES

Question. In developing a human resources system that is mission-centered and performance-focused, how will the creation of open pay ranges and performance pay pools assist the Department in meeting its operational needs?

Answer. A major objective of open pay ranges is to provide DHS management with the flexibility to compete with other employers (private, Federal, State and local), and to attract, hire, and retain the best candidates for positions within the Department. DHS management will have increased flexibility in negotiating employee salaries. Under a pay-for-performance system, the objective is to truly compensate those employees who have made significant contributions to accomplishing the agency's mission. Employees will play a major role in determining their eligibility for performance adjustments based upon their work performance. The intent is to motivate employees to perform their very best; as a result, this incentive should assist significantly in enhancing agency effectiveness and employee retention.

Question. A total of $53 million is included for Max HR in the fiscal year 2006 budget request. What is the total projected cost of the Max HR system?

Answer. The total anticipated cost for the period fiscal year 2005–2008 is $250 million. This amount is broken down as follows:

The total funding includes $43 million for training 100,000 employees, which is essential to ensure that the new HR flexibilities achieve the desired results. This funding will train all Department executives, managers, supervisors, and employees on all aspects of the new system and their responsibilities as leaders in the DHS environment, and to provide the framework for all of the components to work together as one Department of Homeland Security. Comprehensive training also will be provided for HR professionals throughout DHS whose roles and responsibilities are impacted by implementation of the new HR provisions.

Additionally, $56 million in funding will be used for detailed systems design and implementation support and to provide access to experts who are assisting in designing the new DHS performance management system, job evaluation system (including the creation of job clusters), compensation system (including new pay ranges and market pay processes), and linkages for pay and performance. This in-depth expertise is required to ensure DHS creates a program that appropriately links pay, competencies, performance, and labor market, and through this linkage, improves DHS' mission performance and accountability.

$100 million will be required to fund the initial conversion of over 90,000 employees from the General Schedule pay system to newly created market-based pay ranges. This amount will cover one-time conversion costs for employees included in three implementation phases. Phase 1 of the DHS pay conversion, which is scheduled for January 2006, covers employees in DHS HQTRS, S&T, IAIP, OS, U/S MGMT, U/S BTS, FLETC, and EP&R, and is estimated to cost $10 million. Phase 2, which will occur in January 2007, will include U.S. Secret Service and U.S. Coast Guard (civilians). Phase 3, the largest phase covering CIS, CBP, and ICE, will occur in fiscal year 2008.

A total of $9 million is required to fund the new Homeland Security Labor Relations Board (HSLRB) in fiscal year 2005 and 2006. The Board has been established in fiscal year 2005 as an independent entity that will report to the Office of the Secretary. The HSLRB resolves labor-management disputes and is integral to the deployment of the labor relations section of the regulations. $42 million for program management funding is required for program evaluation and to manage appropriate cost, schedule, and control activities at the Departmental level, ensuring that the system investment is managed appropriately and at a good value. Program management funding will provide for earned value management assessments and risk man-

agement. This funding will also ensure the development of a robust metrics and program management evaluation framework that will be used to gauge overall program success. In addition, department-wide communications about MAXHR will be funded from the program management account.

Question. The budget request for fiscal year 2006 includes $10 million to fund the initial conversion of some Homeland Security employees from the General Schedule to newly created market-based pay ranges. Does the Department expect any delays in this conversion to the new system?

Answer. We expect to be on schedule in converting to the new system. DHS employees will be converted to the new pay system in three phases. Phase 1 occurs in January 2006; Phase 2 occurs in January 2007 and Phase 3 occurs in January 2008.

NAC

Question. The budget request provides $26.1 million to continue expansion of the Department's presence at the Nebraska Avenue Complex. What is the Department's estimated timeline for standing up a fully operational Nebraska Avenue Complex?

Answer. We expect to be 70 percent to 80 percent occupied at the NAC within 6 to 9 months of the U.S. Navy vacating the site based on minor renovations to the site as planned and barring any significant infrastructure changes as found during earlier moves within the NAC. The U.S. Navy is expected to vacate the site by December 31, 2005, so we would expect to be 70 percent to 80 percent occupied between May 2006 and August 2006.

We expect to be 100 percent occupied at the NAC within 18 to 24 months (May 2007-October 2007) of the U.S. Navy vacating the site based on the planned major renovations of several buildings at the NAC.

Question. Is there a timeline for the United States Navy to be completely relocated to another facility?

Answer. Yes, December 31, 2005.

Question. Are there projected cost estimates on what the Department will be required to pay for relocation of Navy activities?

Answer. Yes, the original U.S. Navy relocation cost estimates were established between GSA, U.S. Navy, and DHS with OMB review. DHS' share to relocate the U.S. Navy was estimated to be approximately $30,800,000. Of this amount, $12,500,000 was obligated for this purpose in fiscal year 2003 and fiscal year 2004. DHS obligated $12,000,000 year to date in fiscal year 2005 and expects to obligate the remaining $6,300,000 in fiscal year 2005 for a total obligation of 18,300,000 in fiscal year 2005.

FINANCIAL AND PROCUREMENT CONTROLS

Question. What is included in the fiscal year 2006 budget request to improve the CFO's oversight and controls of the Department's bureaus?

Answer. The Office of the Chief Financial Officer (OCFO) fiscal year 2006 budget request includes substantial increases that will enable OCFO to increase its level of oversight and control of the DHS components. OCFO has requested two additional FTEs and $305,000 to increase budget execution oversight of the components. Whereas OCFO conducted mid-year budget execution reviews of the components in fiscal year 2005, the additional staff will allow us to conduct quarterly reviews in fiscal year 2006 and beyond. More staff in the OCFO budget division will allow a redistribution of desk officer portfolios; reduced portfolio sizes will allow all OCFO budget desk officers to work more closely with component budget personnel and to intensify oversight of the components' budget execution. This will allow for more timely identification and resolution of problems in components that require additional oversight. One additional FTE and $152,000 will augment the OCFO's appropriations liaison staff and ensure timelier fulfillment of the appropriations committees' requests.

The request for OCFO also includes five additional FTE and $763,000, and $4,000,000 for technical assistance to implement the DHS Financial Accountability Act. In order to implement the Act, the DHS OCFO will design and implement DHS-wide policy, procedures, and internal controls. The goals of the Act imply that DHS must accelerate consolidation of financial operations. Additional FTE and funding will enable the OCFO to increase financial policy guidance and for OCFO financial analysts and contractors to work closely with the components' financial operations on internal control and standardization projects. Increased interaction will lead to more consistent and better financial performance at DHS.

Question. The budget request proposes funding of $9 million, an increase of $1 million, for the Chief Procurement Officer. As the majority of the funds for this of-

fice have been proposed through the Working Capital Fund, are there sufficient funds for the Procurement Office in the fiscal year 2006 budget request?

Answer. Yes, the fiscal year 2006 increase of $1 million for the Office of the Chief Procurement Officer (OCPO) is sufficient. The OCPO provides acquisition policy, oversight, strategic sourcing, competitive sourcing, integrated systems, and grants policy support for the entire Department. The Office of Procurement Operations, a direct report to the OCPO, is funded separately through the working capital fund and provides operational contracting support to 35 major organizational components including S&T, IAIP, the Offices of the Secretary and Deputy Secretary, and the Under Secretary for Management.

Question. The Department's organizational structure places the Chief Procurement Officer under the Office of the Under Secretary for Management, while other offices like the Chief Financial Officer are funded separately. Would altering this structure to make the Chief Procurement Officer a direct report to the Secretary of Homeland Security help to improve this office's ability to provide oversight to all Department procurements?

Answer. To ensure the administrative functions of the Department are properly integrated, the OCPO should continue to report directly to the Under Secretary of Management and the OCPO's budget should remain a part of the USM budget. Changing the OCPO's reporting structure and/or segregating the OCPO's budget would have no material impact on the Department's ability to provide oversight of the procurement program.

DEEPWATER

Question. Mr. Secretary, the Coast Guard has submitted to Congress a revised baseline of its Deepwater acquisition plan. How confident are you that the Coast Guard has accurately reestimated the use of its assets in this post 9/11 environment?

Answer. The original Deepwater System contracted in 2002 was based on the Coast Guard's 1998 mission demand. I am confident that the revised Deepwater implementation plan reflects the changed requirements of the Deepwater system needed in the post-September 11 environment.

We revised the Deepwater implementation plan based on a comprehensive performance gap analysis that identified new capabilities that the Coast Guard needed to carry out its responsibilities under the DHS Strategic Plan. The original, pre-September 11 Deepwater Program was then modified to incorporate these improved post-September 11 capabilities. The revised plan includes retaining, upgrading, and converting aviation legacy assets as part of the final asset mix and adjusting the program's overall asset delivery schedule to align with operational priorities. The revised plan also includes those capabilities necessary to provide maritime domain awareness and operate successfully in the post-September 11 threat environment. To help ensure the new plan meets broader national and departmental maritime homeland security and interoperability requirements, my staff carefully reviewed and analyzed the revised baseline prior to its approval by the DHS Investment Review Board (IRB). The Department's Joint Requirements Council and IRB also reviewed and approved the plan. The level of analysis and critical thinking that is reflected in the revised Deepwater plan exceeds that of any project that the Department has ever undertaken. For these reasons, I am confident that it will deliver the post-September 11 capabilities needed.

Question. Do you believe there will be further revisions to this plan? If so, why?

Answer. The revised implementation plan provides us with the right mix of assets to ensure its readiness to address current threats. However, the implementation schedule and the planned acquisitions will necessarily adapt to changes in annual appropriation levels and changes in other variables, such as technology upgrades and legacy asset conditions. The revised capabilities and capacities presented within the revised implementation plan are the result of nearly 2 years of analysis, gap assessment, and third party validation after September 11, 2001.

Question. A review of the fiscal year 2003 through fiscal year 2006 budgets indicates that the percent of Deepwater funds spent to sustain legacy ships, aircraft and communications systems climbed each year from 7 percent in the fiscal year 2003 budget to 25 percent in the fiscal year 2006 budget. This is very troubling given that the objective of the program is to reduce the cost of maintaining legacy assets within the Deepwater system. What can be done to reverse this trend and bring new ships and aircraft into the fleet sooner?

Answer. Full support of the President's fiscal year 2006 Deepwater budget request is critical to ensuring urgent legacy asset projects, such as HH–65 re-engining, are funded to immediately correct existing deficiencies while providing significant re-

capitalization funding for procurement of assets to replace those that are rapidly declining.

The Department is taking steps to mitigate legacy asset costs through advancing recapitalization of certain asset classes within the Deepwater program. For example, the fiscal year 2006 Deepwater request includes $108 million to advance acquisition of the Offshore Patrol Cutter by completing the design and purchase of long lead materials for the first cutter. The revised Deepwater plan also advances the acquisition of the Fast Response Cutter.

In addressing legacy asset maintenance issues, the Department has to balance four factors: operational needs, legacy fleet status, current Deepwater acquisition priorities, and available funds. Through sound resource planning and performance assessments we will invest the necessary resources to sustain operational assets until they can be replaced/recapitalized through the Deepwater project.

Question. Is it true that the Coast Guard's major cutters and much of your aircraft fleet are simply beyond their reasonable service life?

Answer. Many Coast Guard legacy assets are aging, technologically obsolete, and require replacement and modernization. The majority of these assets will reach the end of their planned service life by 2010. Coast Guard cutters and aircraft are failing at an alarming rate. However, with proper maintenance and sustainment support, the Coast Guard plans to sustain legacy assets at a level that will allow them to capably perform their missions until they are replaced by their Deepwater counterparts.

The President's fiscal year 2006 Budget requests $966 million for the Deepwater program, which includes critical funding necessary to address immediate legacy asset sustainment issues that threaten the performance of Coast Guard missions, including HH–65 re-engining and the Medium Endurance Cutter Mission Effectiveness Project (MEP). Full support of the President's Budget is critical to sustaining Coast Guard operational performance.

Question. Two years ago, at Congress' request, the Department provided an assessment of the feasibility of accelerating the Deepwater program. At the proposed fiscal year 2006 funding level of $966 million can we expect to accelerate the program?

Answer. The President's fiscal year 2006 Deepwater budget request of $966 million represents a 33 percent increase over the fiscal year 2005 enacted funding level of $724 million. It advances the delivery of the Fast Response Cutter by 10 years and the Offshore Patrol Cutter by 5 years, while beginning the conversion of legacy assets to meet post-September 11 mission requirements. Because of the additional capabilities and revised asset mix included in the revised Deepwater implementation plan, the total program is planned for completion completed in 25 years.

Question. What funding level would be required in fiscal year 2006 and future years to complete the plan within 10 years?

Answer. The President's Budget and the Department support the revised Deepwater implementation plan and the funding stream that acquires it in 25 years at $24 billion. To complete the plan within the next 10 years would require an annual funding stream between $1.7 billion to $2.2 billion per year.

Question. What, if any, improvements in operational effectiveness do you expect once Deepwater is fully implemented?

Answer. The post-September 11 Deepwater system will significantly enhance the Coast Guard's operational effectiveness. The initial Deepwater implementation plan was designed to meet the Coast Guard's missions in 1998. The post-September 11 asset capabilities included in the revised Deepwater implementation plan not only ensure the Coast Guard can meet its new maritime homeland security missions, but also enhance the Coast Guard's ability to meet its traditional mission requirements. Specific operational enhancements contained in the revised Deepwater plan include:

—Improved maritime security capabilities on selected Deepwater cutters, including greater speed, larger flight deck, and automated weapons systems to reduce maritime risk and enhance response to terrorist threats;

—Network-centric command, control, computer, intelligence, surveillance, and reconnaissance (C4ISR) systems to improve maritime domain awareness and interoperability;

—Helicopter airborne use of force and vertical insertion capabilities to provide warning and or disabling fire at sea and in ports, waterways, and coastal regions and to enable the delivery of boarding teams to board and take control of non-compliant vessels;

—Improved long-range surveillance capability to support maritime domain awareness and reduce the maritime patrol aircraft flight hour gap;

—Enhanced all-weather self-defense capabilities on select assets; and

—Improved Chemical, Biological, Radiological, and Nuclear/Explosive threat response on select Deepwater assets.

HH–65 HELICOPTER RE-ENGINING

Question. What is the status of the HH–65 re-engining project? Be specific in terms of how many engines have been replaced.

Answer. In August 2004, the first re-engined HH–65 was delivered to the Coast Guard at Aviation Training Center Mobile, AL, for operational testing and evaluation. As of the September 1, 2005, 10 re-engined HH–65Cs had been delivered for full operational status to Air Station Atlantic City, NJ, (5), Aviation Training Center Mobile, AL, (1), and Air Station Savannah, GA, (4). To accelerate the HH–65 re-engining project the Coast Guard and its contractor, Integrated Coast Guard Systems (ICGS), have examined the quality and suitability of a second re-engining facility located in Columbus, MS. In August 2005, this facility delivered its first re-engined aircraft to the Coast Guard. This aircraft was determined to meet needed quality and suitability parameters and the Coast Guard contracted with ICGS to re-engine an additional 11 aircraft at the Columbus facility. The Coast Guard plans to have all 84 operational aircraft re-engined in early 2007.

Question. Can all the engines be recapitalized within the specified timeframe given the current capacity at Elizabeth City, NC?

Answer. Given the current capacity at Elizabeth City, NC, the re-engining project cannot be completed within the specified timeframe. In order to complete re-engining the operational fleet of 84 helicopters by February 2007, the Coast Guard's Deepwater contractor, Integrated Coast Guard Systems, will rely upon a second re-engining facility at Columbus, MS.

Question. What will have to be done by the Coast Guard to meet the Congressional direction to re-engine the entire fleet within that required 24 month time period?

Answer. Provided the President's request of $133.1 million for HH–65 re-engining in the fiscal year 2006 budget is fully funded, the Coast Guard plans to complete re-engining of the operational fleet of 84 aircraft by February 2007. This is the fastest possible timeline based on the availability of engine kits and parts, increased production at the Coast Guard's Aviation Repair and Supply Center, and additional production capacity at a second facility. ICGS is assessing the quality and suitability of a second facility in Columbus, MS. That facility is now re-engining a single aircraft that is scheduled to be completed in September 2005.

Question. Will a second line be required?

Answer. In order to finish re-engining as quickly as possible and to meet the February 2007 timeline, a second line will be required.

Question. What lessons have been learned from the test helicopter currently being re-engined at the second line which the subcontractor has established at its site?

Answer. It is too early in the process to assess lessons learned. To accelerate the HH–65 re-engining project, the Coast Guard and its contractor, ICGS, are examining the quality and suitability of a second re-engining facility located in Columbus, MS. This facility is expected to deliver its first re-engined aircraft to the Coast Guard in September, 2005. Before making a final determination on the suitability of the facility the Coast Guard is evaluating the second facility's capabilities to control cost, meet schedule requirements, and employ standardized industrial processes.

Question. What value do you see in having a second line outside the Coast Guard's depot-level maintenance facility?

Answer. Using a second production facility will allow completion of the re-engining of all 84 operational HH–65s by February 2007.

Question. What are the challenges of a second line?

Answer. The second facility has not yet been certified as providing a quality product at a reasonable price. Also, as in any lead asset production, there is a substantial learning curve. Other challenges include:

—Validation of capability;
—Cost control;
—Avoidance of schedule delays;
—Parts availability; and
—Standardized industrial process.

COAST GUARD/C–130

Question. In the past, the Defense Appropriations Subcommittee funded the acquisition of 6 new C130Js, which are the next generation beyond the C–130Hs, and began funding to missionize these planes in fiscal year 2005. The President's budget

proposes missionization costs to be borne by the Coast Guard in fiscal year 2006. The cost of these planes has been outside the original Deepwater plan, but now the associated missionization costs are included in the revised Deepwater plan.

What legacy sustainment issues are you experiencing with the C–130H fleet?

Answer. On April 20, 2005, the Coast Guard submitted a legacy asset report to Congress, as directed in the Conference Report accompanying the fiscal year 2005 DHS Appropriations Bill. This report includes the HC–130H AC&I projects that the Coast Guard has included in the fiscal year 2006 budget request and anticipates requesting in future budget submissions. The primary HC–130H sustainment issues are as follows:

APS 137 Surface Search Radar ($75M, cost reflects conversion on 27 aircraft). The Coast Guard's fiscal year 2005 Deepwater budget includes $9 million to start the replacement effort for the HC–130H's APS 137 search radar

Avionics Modernization and Rewiring ($144M, cost reflects 16 aircraft). The HC–130H requires a modernized and supportable cockpit. This cockpit modernization will prepare the aircraft for the inevitable U.S. Airspace restrictions due to increased traffic and the Open Skies policy of route traffic control. Logistically, the aircraft's current cockpit instrumentation will become unsupportable within this decade. With plans for the HC–130H to operate until 2033, this will be a necessary upgrade. Over 500 other DOD aircraft are conducting the same modification. DOD modernization plans will significantly reduce the availability and or support of older parts, resulting in increased repair costs of the existing system.

Center Wing Box Structural Issues. In March 2005, the C–130 manufacturer, Lockheed Martin Aero (LMA), changed the inspection guidelines for C–130 wing boxes based on cracking found in Air Force C–130s of about the same age as some of the Coast Guard HC–130Hs. The wing box problem is not unique to the Coast Guard, but applies to all C–130's world wide. As a result of flight hour limitations and or restrictions identified in LMA Service Bulletin (SB1), the five Coast Guard 1500 series airframes are limited to restricted operations until they are properly inspected over the next 6 months. A second service bulletin is due this month from LMA that will provide the inspection criteria. The estimated cost of completing the 1500 series inspections is $2 million total. The remaining 22 aircraft are newer and will be due for inspections over the next 2 years.

Question. Now that the missionization of the Coast Guard's C–130 fleet is included in the Deepwater plan, what are the future costs to complete this undertaking?

Answer. The Coast Guard plans to have all six C–130J aircraft missionized and available for maritime patrol aircraft work by the end of 2008 at a cost not to exceed $120 million. Funds to complete this missionization were previously provided outside of Deepwater. Additional missionization costs within Deepwater are not currently anticipated. The President's fiscal year 2006 Budget request also includes $5 million to fund the Aircraft Project Office, which manages the C–130J pilot and air crew training, logistics use, and missionization oversight while the aircraft are transitioning to full operational use. As indicated in the fiscal year 2006–2010 Capital Investment Plan (page 116 of the Coast Guard's fiscal year 2006 Congressional Justifications), this cost will recur at $5 million per year through project completion in fiscal year 2008.

Question. Why were these costs omitted in the original Deepwater plan?

Answer. The Congressional Conference Report (H. Rept. 106–710) of June 2000 stated "That the procurement of maritime patrol aircraft (C–130J funded under this heading) shall not, in any way, influence the procurement strategy, program requirements, or down-select decision pertaining to the Coast Guard's Deepwater Capability Replacement Project." Based on this direction the Coast Guard did not include the C–130J in the original Deepwater plan.

Question. Since the acquisition and initial missionization costs of the C–130Js were incurred by the Department of Defense, do you believe that any future costs should also be borne by that Department?

Answer. Department of Defense funding already received in past years is sufficient to complete missionization of the C–130J aircraft. The President's 2006 budget includes a request for $5 million for the Coast Guard to fund the Coast Guard Aircraft Project Office, which will manage the C–130J pilot and crew training, logistics use, and missionization oversight while the aircraft are transitioning to full operational use.

Question. Why shouldn't the Department of Defense continue to complete this effort?

Answer. Funding to acquire and fully missionize the Coast Guard's six C–130J aircraft has already been provided through Department of Defense appropriations. The remaining funds required to complete the project, as outlined on page 116 of

the Coast Guard's fiscal year 2006 Congressional Justifications, should be borne by DHS appropriations since they will be used to train Coast Guard C–130J pilots and crews, fund Coast Guard logistics support, and transition the aircraft to operational use for Coast Guard missions.

RESEARCH AND DEVELOPMENT

Question. Has the Coast Guard R&D program been able to successfully support the Coast Guard's traditional mission areas since the Coast Guard is now an entity under the Department of Homeland Security?

Answer. Yes, the Coast Guard Research and Development program has been able to continue research in non-homeland security (traditional) mission areas. Presently, the Coast Guard is concentrating much of the traditional mission R&D effort on aquatic nuisance species remediation. The Coast Guard is also continuing research and development in other non-homeland security mission areas such as Aids to Navigation, Search and Rescue, Maritime Safety, and Marine Environmental Protection.

Question. How successful has the Coast Guard R&D program been in competing for DHS Science and Technology funding in addition to its own R&D budget?

Answer. The Coast Guard has been successful in competing for DHS S&T funding for homeland security-related projects. In accordance with established S&T protocols, the Coast Guard Portfolio Manager at S&T submits the Coast Guard Maritime Security requirements to the DHS S&T Executive Review Team for evaluation and funding. To date, the Coast Guard has received over $6.5 million of funding from the S&T Directorate in fiscal year 2005.

Question. Do you have any concerns about having this program transferred to the Science and Technology Directorate?

Answer. No, a collaborative relationship between the Coast Guard and the S&T Directorate is both viable and valuable. Integration of funding and research requirements will maximize the effectiveness of both homeland and non-homeland security research.

Question. How can you ensure those Members with concerns about traditional mission research that the Science and Technology Directorate (S&T) will place the same level of consideration on those areas of research as the Coast Guard does?

Answer. Retaining the Coast Guard's capabilities in both homeland and non-homeland security mission areas is of critical importance to DHS. Equally important is the retention of the Coast Guard's research and development capability in both homeland and non-homeland security (traditional) missions. The S&T Directorate is committed to and responsible for supporting the research, development, testing, and evaluation requirements for the entire Department, which includes enhancing the Coast Guard's homeland and non-homeland security mission performance. For example, to date the S&T Directorate has provided $7.56 million toward Project Hawkeye, an initiative that will enhance performance across the entire spectrum of Coast Guard missions by improving Maritime Domain Awareness.

Question. If Coast Guard R&D is transferred into S&T, what role does the Department plan for the Coast Guard Research and Development Center in Connecticut to continue to play in the future?

Answer. The Coast Guard R&D Center is the sole Government entity performing research and development in the area of Aids to Navigation, Search and Rescue, Maritime Safety, and Marine Environmental Protection. The Coast Guard R&D Center will continue to be the critical link to ensure the Coast Guard has the essential research, development, testing, and evaluation requirements to succeed in both its homeland and non-homeland security mission areas.

Question. What follow-on actions is the Coast Guard taking in response to the Congressionally-mandated study of Coast Guard R&D?

Answer. The Coast Guard is taking several of the study's recommendations for action. Key items include: the development and implementation of an overarching Research and Development strategy; continued outreach to other government agencies, industry and academia to establish partnerships; and improved alignment with the Coast Guard Acquisition Program.

COMMUNICATIONS AND TECHNOLOGY SYSTEMS

Question. Why has Rescue 21 been delayed so significantly? The GAO has been very critical of the Coast Guard's acquisition management team known as Deepwater. Isn't this just another example of the Coast Guard not being able to manage large acquisitions?

Answer. Rescue 21's delay in achieving initial operating capability (IOC) is due to problems experienced by General Dynamics C4 System (GDC4S). Those problems

have been twofold in: (a) completing software development needed to integrate the multiple commercial items into a consolidated control interface and (b) resolving performance issues stemming from System Integration Testing (SIT). Software integration and SIT issues have been resolved and the project is ready to enter full rate production upon approval.

The Coast Guard does not consider this delay a result of mismanagement as it has closely followed Coast Guard and DHS acquisition processes, as highlighted by the GAO Report 03–1111 Coast Guard's Rescue 21 Faces Challenges. GAO noted that the Coast Guard has developed key documentation used for managing system requirements and that the Coast Guard has a system in place for identifying, prioritizing, and minimizing risks.

The Coast Guard has successfully managed and executed several comparable acquisitions in the past. Recent projects such as Seagoing Buoy Tenders ($618 million), Coastal Patrol Boats ($327 million), and the Great Lakes Icebreaker ($140 million) were each remarkably successful. The Coast Guard will continue to seek out process improvements and apply past lessons learned to manage the Rescue 21 acquisition.

Question. Please provide an update on achieving full operating capability. What capabilities will Rescue 21 have at the end of fiscal year 2006?

Answer. Provided Rescue 21 is funded consistent with the Coast Guard's Capital Investment Plan outlined on page 116 of the Coast Guard's fiscal year 2006 Congressional Budget Justification, the Coast Guard expects Rescue 21 to reach full operating capability in fiscal year 2007. At the end of fiscal year 2006, deployment of Rescue 21 to all continental U.S. coastal regions will be complete.

Question. When will Rescue 21 transition to replace the National Response Distress System (NRDS), which is being supplanted by Rescue 21?

Answer. The Rescue 21 system will be deployed incrementally in all Coast Guard Sector/Group Regions. Following deployment and testing within each Coast Guard Sector/Group Region, the legacy NDRS in the affected region, will be removed and the Rescue 21 system will become operational. Nationwide deployment is expected to be complete in fiscal year 2007.

Question. When is NRDS expected to come offline?

Answer. The Rescue 21 system will be deployed incrementally in all Coast Guard Sector/Group Regions. Following deployment and testing within each Coast Guard Sector/Group Region, the legacy NDRS, in the affected region, will be removed and the Rescue 21 system will become operational. Nationwide deployment is expected to be complete in fiscal year 2007.

Question. Please provide an update of your planned Vessel Tracking System installation recapitalization schedule. When will the project be completed?

Answer. The Ports and Waterways Safety System (PAWSS) installation/recapitalization has been completed in five ports with two additional ports to be completed in the fourth quarter of fiscal year 2005, pending completion of remote site leases. Project closeout and transition of all systems to long-term operations and support will occur by the end of fiscal year 2006. Automatic Identification System (AIS) capability, which is an integral part of PAWSS, has been installed in all nine scheduled Vessel Traffic Service (VTS) ports.

Question. How will funding interruptions affect the project schedule, for instance, if funding is not provided in fiscal year 2006 what will not get done?

Answer. VTS systems in Puget Sound and San Francisco will not be recapitalized with funding provided to date. The Coast Guard's fiscal year 2006 Unfunded Priorities List includes $17 million for the PAWSS, the funding required to complete VTS recapitalization in these ports.

Question. Please provide an update on the progress/status of implementation of the nationwide Automated Identification System (AIS), especially as it relates to the maintenance of the Coast Guard's common operating picture.

Answer. The Nationwide AIS project has been approved and chartered by the DHS. The project is in the requirements and planning phase of the acquisition process.

Concurrently, numerous initiatives are underway to provide prototype and interim AIS capability to provide AIS data to the National Maritime Common Operational Picture (COP). The progress to date includes:

—Installation of AIS capability at all Vessel Traffic Services (9 sites).

—Deployment of receive-only AIS sites in key locations in Alaska (8 of 11 AIS sites).

—Deployment of 4 prototype AIS receivers on National Oceanic Atmospheric Administration weather buoys to provide AIS tracking of vessels offshore of the United States.

—AIS receiver installations for research & development purposes:

—On Oahu that provides extensive coverage of the major Hawaiian Islands;
—In San Francisco Bay, CA;
—In Miami, Port Everglades and Key West, FL; and
—In Long Island Sound, Cape May NJ, and the Cape Cod Canal.
—Installation of AIS sites on offshore platforms in the Gulf of Mexico to monitor traffic inbound to Gulf ports (3 of 4 planned AIS sites installed).
—Deployment of AIS receiver as part of a concept validation on a low earth orbit satellite for long-range AIS vessel tracking to be launched in the second and third quarter fiscal year 2006.

Question. How does AIS implementation fit with Ports and Waterways Safety System (PAWSS) and Rescue 21?

Answer. The Coast Guard, thru the PAWSS project, has deployed AIS capability in all nine VTS areas. Rescue 21 replaces the Coast Guard's antiquated short range command and control communications systems and it does not include AIS. The Nationwide AIS project will share infrastructure with Rescue 21 wherever site and technical compatibility will allow, e.g., towers.

Question. How is it different from PAWSS?

Answer. The AIS is a cooperative vessel tracking system whereby vessels transmit their position, identification, speed, course, cargo, and other information to vessels in their area and shoreside receivers within range of the system. The Maritime Transportation Security Act of 2002 specifies AIS carriage requirements for certain vessels navigating U.S. waters. The Nationwide AIS project will implement necessary infrastructure to receive AIS transmissions from shipboard systems and distribute this data to the Coast Guard's Common Operational Picture to enhance maritime domain awareness.

The PAWSS project was established to build new Coast Guard Vessel Traffic Service (VTS) systems and to modernize and recapitalize existing ones. The Coast Guard operates VTS in nine U.S. ports to provide traffic information, traffic organization, and navigation assistance services necessary to fulfill the Coast Guard's statutory maritime safety and environmental protection responsibilities under the Ports and Waterways Safety Act of 1972. PAWSS/VTS employ AIS, among other surveillance systems to monitor and access information on vessel movements within a VTS area.

A table highlighting the basic tenants of each project is provided below:

Compare/Contrast	Nationwide AIS	PAWSS
ACRONYM	Automatic Identification System	Ports and Waterways Safety System
Primary User	U.S. Coast Guard, Commercial vessels.	U.S. Coast Guard, Commercial vessels
Focus	Pre-9/11—Safety: for ship to ship to communicate rules of the road. Post-9/11—Safety and Security—Maritime Domain Awareness (MDA).	Pre-9/11—Safety Post-9/11—Safety and Security (Maritime Domain Awareness)
Purpose	Track vessels approaching, entering, and transiting U.S. navigable waters.	Manage vessel traffic in nine U.S. ports
Project	Enhance the nation's maritime domain awareness, safety, and security.	Provide Vessel Traffic Service
Line of Sight Transmissions	Send and receive: Data, ship-to-ship, ship-to-shore, shore-to-ship.	Send and Receive (& share): Voice & Data, AIS-based; radar & cameras
Location	Ports, waterways and coastal areas out to 2000 nautical miles via towers, buoys, offshore platforms, e.g., oil rigs, & satellite(s).	9 U.S. ports: one each in AK, NY, MI, CA, WA; two each in LA and TX

Question. Is PAWSS still needed or is it being phased out?

Answer. The PAWSS, as an acquisition project, is being phased out. The Coast Guard established PAWSS as an acquisition project to build new Coast Guard VTS and modernize existing systems. The PAWSS project resulted in two new VTS's, recapitalized five of the existing VTS's completely, and partially modernized two others (Puget Sound, WA and San Francisco, CA).

While there will be no more acquisitions completed through the PAWSS project, the Coast Guard VTS will still operate, providing navigation services and ensuring safety and environmental protection of U.S. waters as required by the Ports and Waterways Safety Act of 1972.

Question. How is AIS different from Rescue 21?

Answer. The AIS is a cooperative vessel tracking system whereby vessels transmit their position, identification, speed, course, cargo, and other information to vessels in their area and shoreside receivers within range of the system. The Maritime Transportation Security Act of 2002 specifies AIS carriage requirements for certain vessels navigating U.S. waters. The Nationwide AIS project will implement necessary infrastructure to receive AIS transmissions from shipboard systems and distribute this data to the Coast Guard's Common Operational Picture to enhance maritime domain awareness.

The Rescue 21 project will replace the existing and obsolete National Distress and Response System (the system used by the boating public to hail the Coast Guard when in distress) and provide the Coast Guard with a modern coastal command, control, and communications system. Rescue 21 will be capable of monitoring the international VHF–FM distress frequency to improve search and rescue response operations and communications with Coast Guard and other Federal, state, and local first responders and commercial recreational boats.

A table highlighting the basic tenants of each project is provided below:

Compare/Contrast	Nationwide AIS	Rescue 21
ACRONYM	Automatic Identification System	Formerly: National Distress and Response System (NDRS)
Primary User	U.S. Coast Guard, Commercial vessels.	U.S. Coast Guard, commercial, boating public
Focus	Pre-9/11—Safety: for ship to ship to communicate rules of the road. Post-9/11—Safety and Security—Maritime Domain Awareness (MDA).	Pre-9/11—Primary—Safety Secondary—support all other CG/DHS missions post-9/11—same
Purpose	Track vessels approaching, entering, and transiting U.S. navigable waters.	Command, control, and communication system to allow USCG to hear and locate mariners in distress
Project	Enhance the nation's maritime domain awareness, safety, and security.	Modernize the USCG's legacy NDRS
Line of Sight Transmissions	Send & receive: Data, ship-to-ship, ship-to-shore, shore-to-ship.	Send and receive: Voice and Data
Location	Ports, waterways and coastal areas out to 2000 nautical miles via towers, buoys, offshore platforms, e.g., oil rigs, & satellite(s).	Towers and vessels in 46 regions throughout the United States, including Guam and Puerto Rico

FEDERAL LAW ENFORCEMENT TRAINING CENTER (FLETC)

Question. Mr. Secretary, as you complete your top to bottom review of the Department, what emphasis will you place on the need to provide basic and advanced training to law enforcement personnel at the Federal Law Enforcement Training Center?

Answer. Standardized, high quality training is an exceptionally critical component in the success of the DHS responsibilities. The Federal Law Enforcement Training Center (FLETC) is the government's principal provider of interagency law enforcement training and is DHS's primary source for intradepartmental law enforcement training. FLETC already has accelerated the number and types of training programs being offered in concert with its Partner Organizations since the September 11, 2001, terrorist attacks. While basic training continues to be the first scheduling priority for FLETC, there has been a greater emphasis placed upon relevant advanced training to meet the post-September 11 focus on security of the homeland. FLETC has undertaken an initiative for Counterterrorism and Practical Applications Training, which provides hands-on experience for trainees at all levels to handle first responder situations, prevention and appropriate follow-up investigative

measures. Further, FLETC has a major role in international, State and local training with an emphasis on strengthening coordination with Federal law enforcement entities, to include intelligence sharing training. Under DHS's auspices, the Department anticipates relying heavily upon the enhanced and innovative training and increased physical plant capacities now available at the four FLETC sites in Charleston, SC; Cheltenham, MD; Artesia, NM and Glynco, GA.

Question. Do you anticipate opportunities for cross-training of law enforcement personnel?

Answer. One of the principal reasons for the creation of DHS is to continuously improve the overall cooperation, coordination information sharing and interoperability of law enforcement components at all levels related to security for the United States. To help bring about this improvement, DHS is encouraging greater measures that are intended to breakdown traditional organizational and cultural barriers. Cross-training and shared training experiences of multiple agencies is becoming more the norm. FLETC's approach to consolidated training, which emphasizes common understanding and cooperation through mixed class association, affords agencies the opportunity to benefit from mutual experiences. Many of FLETC's basic and virtually all of its advanced programs are scheduled to accommodate multiple training organizations. In the area of counterterrorism training, subjects such as weapons of mass destruction, critical infrastructure, crisis management and land and seaport security are open to all agencies with those needs. These include DHS, Department of Justice, Department of Defense and many others across the spectrum of law enforcement. DHS expects to expand and enhance training that is relevant and contemporary to the evolving needs of all agencies that are involved with the homeland security.

Question. Mr. Secretary, will your assessment examine the various training facilities owned or used by Departmental entities to ensure that they are being fully utilized and not duplicative of each other?

Answer. Training facilities, per se, were not themselves a specific focus of the review. Training has several different elements in DHS, from the general training of our employees, to our law enforcement academy, and to our training centers for first responders. Our plan brings together DHS' key preparedness programs, including first responder training programs. The U.S. Fire Administration and the Noble Training Center are moved into a new Preparedness Directorate, along with the training programs such as those at Ft. McClellan. The purpose for creating this Directorate, and for pulling these programs together, is to give our existing preparedness efforts—including training and exercises—a focused direction. With these programs in one Directorate, DHS will be in a better position to ensure that they are being fully utilized without being duplicative.

Question. Mr. Secretary, the war on terror requires a new approach to training law enforcement personnel. Do you foresee the need to provide new types of training infrastructure or counterterrorism training facilities that mirror our existing vulnerabilities?

Answer. Yes, the future operating environment of DHS will include continuing and increasingly sophisticated terrorist threats to our nation. Post-September 11, the FLETC, the primary law enforcement training organization for the DHS, began vigorously reviewing its training programs and developing and/or revising programs and facilities as appropriate to better prepare agents and officers in executing their duties in the Global War on Terrorism. The FLETC developed a plan and is currently in the planning design and execution construction phase for this type of infrastructure. The practical application counterterrorism training facility design is based on the FLETC and its Partner Organizations expertise on anti/counterterrorism operations and related training requirements to defeat terrorism. The FLETC offers the most current law enforcement training curricula available anywhere and has the instructional experience and expertise to meet the challenges set forth by our adversaries. However, to accentuate our training and meet these challenges, we continually upgrade our tactical facilities and construct training facilities that are responsive to the stated needs of the agencies engaged in the war on terrorism. The FLETC trains officers and agents from 81 Partner Organizations. It is imperative that we attempt to replicate the types of environments that our officers will surely encounter, to enhance their probability of survival and the success of guarding our homeland.

Consolidated training, the concept on which the FLETC was established, allows agencies with divergent missions to train together, in a consistent manner. This proposed training facility will meet the Department's primary goals to prevent terrorist attacks, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. This initiative represents the proactive "imagination," cited in the 9/11 Commission's report, needed to combat terrorism effectively.

The FLETC and DHS have been called upon by the Military to provide up-to-date Counterterrorism training. As the Military's mission changes, they have been expected to perform more like a Law Enforcement Officer rather than a soldier. The urban environments and circumstances that our soldiers face replicate the Use of Force decisions that our police officers face everyday. This mission change has forced the necessity for greater interaction between Law Enforcement and the Military. The FLETC has and continues to be a willing partner in meeting these challenges.

QUESTIONS SUBMITTED BY SENATOR THAD COCHRAN

AVIATION SECURITY

Question. The Department's inspector general released a report yesterday stating that there has been a lack of improvement over the last year in detecting dangerous items—including guns, knives, explosives—at airport security checkpoints. What role will next generation detection systems play in improving airport security?

Answer. TSA has designed its passenger checkpoint technology portfolio to incorporate solutions that will help improve explosives and weapons detection at its checkpoints. The next generation of checkpoint technology will automate the detection of explosives that might be concealed on an individual's body, as well as within the carry-on baggage/items they are carrying. Additionally, TSA is exploring body imaging technologies that will allow screeners to detect weapons (metallic and non-metallic) and explosives that an individual might attempt to hide on their person.

Question. Pilot programs at our airports play a critical role in moving technology from the research stage to practical deployment. What is the status of pilot programs for aviation security checkpoint detection technology, and when will these pilot programs begin?

Answer. TSA has initiated a number of operational testing and evaluation pilot projects involving the next generation of checkpoint technologies to expand TSA's explosives detection capabilities. Highlights from ongoing pilot programs are as follows:

Explosive Trace Portals (ETP).—TSA has deployed 15 ETPs to 14 airports nationwide to evaluate their operational efficiency and effectiveness for screening passengers for explosives. These pilots have been initiated at the following airports and are scheduled to continue through summer 2005: Rochester, NY; JFK, NY; Gulfport, MS; Baltimore, MD; Jacksonville, FL; Phoenix, AZ ; Miami, FL; Providence, RI; Las Vegas, NV (2 units); Los Angeles, CA; San Francisco, CA; Boston, MA; Tampa, FL; and San Diego, CA. TSA has allocated $28.3 million for the purchase and installation of additional trace portals in fiscal year 2005.

Explosive Trace Detection Document Scanners.—TSA is operationally testing and evaluating an explosives detection document scanner at 4 airports: Ronald Reagan Washington National (DCA), Los Angeles International (LAX), John F. Kennedy International (JFK), and Chicago O'Hare International (ORD). The current technology requires that the screener manually handle the travel document to obtain the sample needed for analysis to determine if traces of explosives are present. Based on the preliminary results of the pilot at the four airports, TSA has determined that an automated solution better suits operational and security needs. Consequently, the project has been refocused to develop a technology solution that will meet those needs. A pilot project for the automated prototype will be scheduled as soon as that product is determined ready for an operational test and evaluation.

Question. There is a critical need to identify new and emerging technology, in addition to explosive detection systems, to provide enhanced security protections at our nation's airports. Could you tell us what other progress the Transportation Security Administration (TSA) has made in identifying appropriate technology to improve the security and efficiency of the current airport passenger screening process?

Answer. In addition to the operational test and evaluation pilots underway using explosives detection trace portals and explosives detection document scanners, TSA has a number of R&D projects underway to expand both weapons and explosives detection capabilities. These projects include, but are not limited to:

—*Whole Body Imaging Technology.*—TSA continues to examine the feasibility of using a whole body imaging technology to improve the detection of explosives and prohibited items on persons. Ongoing efforts with two vendors has led to the development of a device that is capable of producing a generic body image that effectively highlights security threats on persons while not unduly infringing on their privacy. TSA is currently working on the details for the pilot phase,

including vendor capabilities to support a timetable, selection of the pilot locations, and the operating policy for screening with this technology.

—*Explosives Detection System (EDS) for carry-on baggage.*—TSA has conducted preliminary evaluations of an automated EDS for carry-on baggage and is currently collecting engineering data with the unit to promote further development. This technology will automate the detection of explosives in carry-on baggage, similar to the capabilities TSA has achieved for checked baggage screening. Simultaneously, we have a robust ongoing R&D project to develop a technology that will automate the search not only for explosives in carry-on baggage, but for weapons as well.

—*Cast and Prosthetic Device Scanner.*—TSA is working to develop a technology solution to more effectively screen cast and prosthetic devices for weapons and prohibited items. TSA expects to pilot the technology in the first quarter of fiscal year 2006.

—*Explosives Detection Bottle Scanners.*—TSA is working with industry to evaluate the effectiveness of bottle scanners to screen for liquid explosives. TSA has issued a solicitation to industry to submit products for lab evaluation.

NATIONAL CENTER FOR CRITICAL INFORMATION PROCESSING AND STORAGE

Question. The National Center for Critical Information Processing and Storage at Stennis Space Center performs the important function of providing a secure and reliable system to process, manage, and secure data for the Federal Government. Could you update us on the status of that project?

Answer. Construction of the DHS data center at Stennis Space Center has been delayed. The Naval Oceanographic Office had been experiencing difficulties issuing a construction contract prior to Hurricane Katrina. The Naval Oceanographic Office now reports that, due to Hurricane Katrina, work crews are not available for the limited construction effort that is under contract (demolition and roofing). The delay to the project is not yet fully quantifiable. The DHS construction effort must now compete for resources with regional reconstruction efforts.

Question. Specifically, when will the additional $30 million of fiscal year 2005 be available for build-out and construction at Stennis?

Answer. The Stennis Procurement Package was released by DHS on May 13, 2005.

QUESTIONS SUBMITTED BY SENATOR TED STEVENS

TRANSPORTATION OF BUTANT STOVES (WITHOUT BUTANE) ON AIRPLANES

Question. Constituents have contacted me to complain about TSA. Alaskans have attempted to carry on butane stoves onto airplanes within their luggage. The stoves, although no butane was present, were confiscated by TSA. These stoves are used for camping and general use in rural Alaska; the stoves do not pose a threat to anyone on a plane.

Why is TSA disallowing passengers from carrying butane stoves, without butane, in their luggage?

Answer. Under regulations issued by the Federal Aviation Administration (FAA), there are restrictions in place on the transport of hazardous materials on board any aircraft. With regard to the transportation of butane stoves as checked baggage, in accordance with the baggage screening standard operating procedure (SOP), if a TSA screener finds a stove that potentially has fuel inside, an airline employee is notified so that a determination may be made regarding the contents of the stove. Typically, the airline employee removes the fuel bottle(s) from the stove, after which the stove can be transported in checked baggage. If the fuel bottle cannot be removed, in general, it will not be allowed to be transported. In some small locations in Alaska where the transport of camp stoves is prevalent and it is relatively easy to contact the passenger, the airline employee will contact the passenger and give that person the option to empty and clean the bottle before accepting the stove for transport. However, an unused camp stove still in the box with no fuel or emanating fumes should not be refused transport.

FISHERIES ENFORCEMENT

Question. I'm informed the Coast Guard plans to deploy C–130s to Shemya or Galena to increase surveillance and enforcement of fisheries laws inside the Maritime Boundary Line. A report issued in 2004 indicated the Coast Guard could not render its deployment throughout the high threat season because of the lack of facilities in the Aleutians. Last year, I included language in the Homeland bill to direct the

Coast Guard to include in its budget submission the funds necessary to provide support facilities for Shemya, Galena, Cold Bay and other western Aleutian Islands. The Coast Guard was not able to follow Congressional direction and the costs were not included in the budget submission.

What are the costs estimates associated with this problem?

Answer. Increased regulation and management on the Russian side of the Maritime Boundary Line (MBL) have significantly decreased the need to forward deploy C–130 aircraft for MBL patrols. MBL enforcement flights originating from Air Station Kodiak are proving effective. At the same time, the need for forward-deployed HH–60's appears to be increasing to meet search and rescue and fisheries enforcement mission needs in Western Alaska waters.

HH–60 forward deployments often occur from locations such as Dutch Harbor, Cold Bay and St. Paul Island. Although highly effective, these forward deployments often present our crews with challenging conditions because of sub-standard facilities—and inadequate commercial infrastructure to properly support these deployments. Addressing these deficiencies is a Coast Guard priority.

The Coast Guard recently initiated a formal planning effort to develop alternatives and identify resources needed to respond to these changing mission needs. Most of these facilities are not Coast Guard-owned, so innovative public-private partnerships may be necessary to allow infrastructure improvements. The Coast Guard will keep the Committee advised of progress on this planning effort. The Coast Guard can not accurately predict costs at this early stage in the planning process.

UAVS

Question. What are the Coast Guard's plans for using Predator medium endurance unmanned aerial vehicles for fisheries enforcement and search and rescue activities in Alaska?

Answer. The Coast Guard has no immediate plans to use Predator unmanned aerial vehicles (UAVs) for operational service in Alaska. The recent proof of concept exercise demonstrated promise for a maritime-configured UAV, but identified shortcomings must be addressed to make this a Coast Guard mission capable asset. Among the technical challenges that still must be resolved are reliable communications and aircraft control at high latitudes, integration of on-board sensors, limited all-weather operations (including icing and crosswind limits), and compliance with Federal Aviation Administration air control requirements.

UAVs remain a critical future element of the Coast Guard's Deepwater program. The Coast Guard is partnering with other DHS and DOD agencies to carry out further evaluation programs and take advantage of technology improvements that will ultimate make UAVs suitable for use in the maritime environment.

Question. Does the Department plan to utilize the two previous Alaskan UAV demonstrations for further testing in Alaska or Hawaii?

Answer. DHS is working with the DOD to plan additional UAV testing in all operational environments to demonstrate the UAV concept to support a variety of missions. A cooperative effort between the National Oceanic and Atmospheric Administration (NOAA) and the Coast Guard to test UAV use in Hawaii, combining scientific research with maritime sensor validation, was recently cancelled due to lack of NOAA funding. The Coast Guard will continue to establish partnerships that may yield opportunities for future Hawaii-based testing.

Further demonstrations in Alaska can be planned when UAV technology matures to resolve the key issues of reliable communications and aircraft control at high latitudes and all-weather operations (including icing and crosswind limits). Prior Coast Guard UAV testing in Alaska has demonstrated that these limitations restrict UAV operations in Alaska.

Question. Does the Department have any plans to use UAV's to help TSA provide surveillance to non-aviation modes of transportation such as the Trans Alaska Pipeline System?

Answer. UAVs offer a range of capabilities that are suitable throughout DHS. The UAV capability for 24-hour, all weather surveillance is particularly useful in border security applications, critical infrastructure protection, transportation security, or in support of U.S. Coast Guard (USCG) maritime domain awareness missions. In April 2004, the DHS/UAV working group submitted a report to Congress addressing the applicability of UAVs in various homeland security applications.

As part of a USCG Predator 2 UAV demonstration in July 2004, TSA coordinated with the USCG to fly over designated sites on the Trans Alaska Pipeline (TAPS). The purpose of the TAPS demonstration was to evaluate the effectiveness and practicality of the UAV and associated sensors for pipeline surveillance. This effort pro-

vided additional evidence of the utility of UAVs as part of a layered surveillance effort. TSA will continue to evaluate the use of UAVs with regard to pipeline surveillance and looks forward to working with Congress on the issue.

QUESTIONS SUBMITTED BY SENATOR PETE V. DOMENICI

BORDER NEEDS—SECURITY UPDGRADES AT PORTS

Question. America has 197 land ports of entry, and it has been almost 20 years since we launched a major effort to upgrade infrastructure at those ports. That last effort occurred in 1986, when former Senator DeConcini and I developed the Southwest Border Improvement Program to improve border infrastructure so that States could better take advantage of commerce and trade opportunities with Mexico. That was almost 15 years prior September 11, 2001.

Since September 11, we have placed increasing emphasis on upgrading security for our airports, seaports, and critical infrastructure. It is imperative that we also improve land port security. To that end, I will introduce a bill authorizing additional funds for investment in our nation's border crossings.

Have you considered what kinds of improvements are necessary at our land ports of entry and how much these upgrades might cost?

Answer. DHS is in the midst of a systems-level review of its border control architecture to identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border. DHS will identify a program manager to oversee the development of a specific set of border security plans. The Department will be in a better position to comment on this question following the conclusion of this review.

Question. Specific improvements are needed at the Columbus port of entry in New Mexico, and the General Services Administration (GSA) has proposed construction on the Columbus project to begin in 2007 or 2008. Do you support GSA's recommendation and will you make every effort to keep the project on track for construction?

Answer. As noted above, DHS is in the midst of a systems-level review of its border control architecture. This review is intended to help the Department identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border. The Department will be in a better position to comment on this question following the conclusion of this review.

BORDER NEEDS—UAV TECHNOLOGY

Question. In last year's intelligence reform bill, I called for the Department of Homeland Security to develop a plan for using Unmanned Aerial Vehicles ("UAVs") on America's southwest border.

In New Mexico, we have some experience with UAVs because our university near the southwestern U.S. border operates a UAV validation and test facility sponsored by the Department of Defense. Because of the established presence of UAVs at New Mexico State University, and because of our location as a border state, I believe New Mexico would be an asset in the use of UAVs for surveillance.

What are your views concerning the use of UAVs for securing remote areas of our borders?

Answer. As noted above, DHS is in the midst of a systems-level review of its border control architecture. DHS is also currently working to begin the process of procuring UAVs. The Department's objective is to get that done in a matter of months and start to deploy UAVs and have them flying over the border. That said, DHS cannot rely exclusively on UAVs, and manned vehicles and helicopters will also play a role.

Question. How many UAVs does DHS currently own?

Answer. As of August 20, DHS currently does not own any UAVs.

Question. Where are these UAVs stationed?

Answer. As of August 20, DHS currently does not own any UAVs.

Question. Will your staff evaluate evaluate the existing UAV facility at New Mexico State University and the Las Cruces International Airport as a potential home for the Department's UAV program?

Answer. As noted above, DHS is in the midst of a systems-level review of its border control architecture. The Department will be in a better position to comment on this question following the conclusion of this review.

BORDER PERSONNEL—MANPOWER

Question. As you know, adequate staffing at our nation's land ports of entry is essential for the safety of parties involved in the flow of traffic across the border and for efficient commerce.

Last year's legislation that reorganized our intelligence community called for an increase in border patrol agents, and President Bush's fiscal year 2006 budget requests funds to hire an additional 210 agents.

Have you studied where placing these agents would be most beneficial?

Answer. Emergency Supplemental Legislation and President Bush's fiscal year 2006 Budget call for the hiring of an additional 710 agents by the end of fiscal year 2006, and CBP is taking aggressive steps to recruit, hire and train candidates to fill these spots. The hiring of these new agents comes in addition to the standard attrition hires that supplement the several hundred agents who retire, transfer, or leave for medical reasons over the course of a year. New agent positions will be allocated based on risk-based priorities.

Question. When might these new agents be hired and put in place?

Answer. There is currently an open recruiting announcement to obtain additional potential new employees.

Question. How can we better retain existing border patrol officers so that as we place these new agents along our borders, we are not losing agents with experience?

Answer. CBP is currently examining methods that can be used to retain seasoned agents. The current attrition rate for experienced agents (GS–9 and higher) is less than 5 percent.

BORDER PERSONNEL—TRAINING AT FLETC

Question. One of the Federal Government's premier training sites for law enforcement officers is located in New Mexico. Many Federal law enforcement officers have trained at the Federal Law Enforcement Training Center in Artesia (FLETC-Artesia), including Air Marshals and Federal Flight Deck Officers.

Additionally, both basic and advanced training for Border Patrol Agents is now conducted at FLETC-Artesia. I lauded the Department's decision to consolidate border patrol training in Artesia because it makes sense to have all training at one facility. Additionally, training border patrol officers in a border State gives trainees a first-hand look at the area they are charged with protecting.

What, if anything, does the Department need from FLETC-Artesia?

Answer. FLETC is proceeding to put into place the temporary structures and staffing directed in the recently enacted fiscal year 2005 Supplemental. As more information and details are developed on additional training needs we will keep the Congress apprised.

Question. Has DHS considered taking border patrol trainees to the Mexico border as part of their overall training?

Answer. FLETC uses scenario base training utilizing Spanish speaking role players in a controlled environment identical to that seen on the southwest border. This scenario based training affords trainees the opportunity to correct mistakes and become comfortable with assigned duties prior to assignment in a U.S. Border Patrol sector. This system of training is more flexible and less costly than providing visits during basic training to border sites. The Border Patrol also employs a system of supervision and on-the-job experience for newly graduated agents.

Question. If new facilities were constructed at FLETC-Artesia, would you support legislative language to streamline the design, engineering and construction of those facilities?

Answer. The Department is always open to considering legislative methods that streamline and improve our processes while promoting full and open competition.

NEW MEXICO CAPABILITIES—TRAINING AT PLAYAS

Question. Secretary Chertoff, last fall New Mexico Tech opened the Playas Training Center. DHS played an integral part in this center by providing the funding for New Mexico Tech to purchase Playas, a small town in Southwest New Mexico that was virtually abandoned when the copper smelting operation in the area was shut down in 1999.

Playas' remote location and open space makes it an ideal place for New Mexico Tech to develop a wide range of research and training activities to support homeland security efforts nationwide.

What new training activities could DHS use at Playas?

Answer. It is my understanding that Playas will be jointly developed by the New Mexico Institute of Mining and Technology and the New Mexico State University.

As you are aware, ODP has funded the New Mexico Institute of Mining and Technology since fiscal year 1998 as part of the National Domestic Preparedness Consortium. As part of the Consortium, the New Mexico Institute for Mining and Technology supports ODP's mission of assisting State and local governments plan and prepare for incidents of domestic terrorism by providing critical training to the Nation's first responders. The State of New Mexico used State funds rather than Federal homeland security funds to purchase the Playas Training Center. Nevertheless, ODP does have a use agreement in place with New Mexico Tech to use the Playas Training Center over a 5-year period. As the Playas Training Center is further developed, the Department's ODP will coordinate with New Mexico Tech officials to determine the types of training initiatives that could be supported by the Playas Training Center.

Question. How much is included in the President's fiscal year 2006 budget for training first responders?

Answer. The fiscal year 2006 President's Budget request for SLGCP includes over $83 million for the State and Local Training Program. Through this funding, SLGCP will continue to develop and deliver state-of-the-art training programs through its coalition of "Training Partners." This coalition, comprised of government facilities, academic institutions and private organizations provide a variety of specialized training for emergency responders across the country. The fiscal year 2006 funding request will support SLGCP's Continued and Emerging Training Program, the Center for Domestic Preparedness, and the National Domestic Preparedness Consortium. In addition, a portion of SLGCP grants to States and urban areas are also devoted to training.

FEMA also conducts an extensive array of training for emergency personnel through the National Fire Academy, the Emergency Management Institute, and the Noble Training Center with a budget that totals approximately $15 million. Other DHS components, such as the Federal Law Enforcement Training Center, also provide training for selected State and local personnel.

Question. What are your thoughts on providing standardized training for all first responders, at both the Federal and local level, in a facility like the one at Playas?

Answer. The New Mexico Institute of Mining and Technology, including its training facility at Playas, already supports ODP's training efforts through the National Domestic Preparedness Consortium. As such, these facilities will comply with all training standards required for ODP training.

Standards for training encompass the instructional design of the training, the quality of training content, the effectiveness of the instructors, as well as successful knowledge transfer measured through student evaluation. With respect to development of training programs, the ODP Training Division has adopted the industry standard instructional systems design approach of analysis, design, development, implementation, and evaluation (ADDIE) as detailed in the ODP Strategy for Blended Learning. The ADDIE approach for instructional design ensures a valid training need is identified, the most effective methodology for instruction is identified, and training content is monitored for accuracy and effectiveness throughout the process.

The development of training content based on effective needs analysis is also based upon performance standards. DHS efforts in this area related to training for emergency responders began with the ODP Training Strategy developed in 2002, which provided guidance on who should be trained to perform what tasks, using what methodologies to maximize training efficiencies. The strategy further addressed effective methods for evaluating competency and performance after training was completed and what gaps needed to be remedied. This work led to the ODP-developed Emergency Responder Guidelines, which were promulgated in August 2002. These are currently undergoing revision to reflect a broader range of response disciplines and the private sector.

Additionally, as the executive agent for the development and implementation of HSPD–8, "National Preparedness," SLGCP has developed and promulgated an Interim National Preparedness Goal (NPG). The Interim NPG, which was released on March 31, 2005, was developed using capabilities-based planning. Capabilities are combinations of resources that provide the means to achieve a measurable outcome resulting from performance of one or more critical tasks, under specified conditions and performance standards. The Target Capabilities List identifies 36 Target Capabilities and is currently available.

ODP's Training Division, along with our training partners, is in the process of examining the capabilities associated with the national priorities included in the Interim National Preparedness Goal to align training curricula to these national priorities and the related capabilities. It is the Department's goal and expectation to have its training courses aligned with the national priorities in fiscal year 2006.

Further, with respect to professional standards, ODP requires its training partners, State Administering Agencies, and Federal partners to adhere to and incorporate the following professional standards in training curricula to which they are applicable:

—29 Code of Federal Regulation (CFR)1910.120, Hazardous Waste Operations and Emergency Response;
—29 CFR 1910.134, Respiratory Protection;
—National Fire Protection Association (NFPA) 471, Recommended Practice for Responding to Hazardous Materials Incidents;
—NFPA 472, Professional Competence of Responders to Hazardous Materials Incidents;
—NFPA 473, Standard for Competencies for EMS Personnel Responding to Hazardous Materials Incidents;
—NFPA 1006, Standard for Rescue Technician Professional Qualifications;
—NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs 2004, specifically Chapter 5, section 5.12; and
—NFPA 1670, Standard on Operations and Training for Technical Rescue and Search Incidents.

Question. Will the Department work to make State homeland security directors aware of the Playas Training Facility in an effort to help local first responders receive adequate training?

Answer. ODP is undertaking a web-based information portal initiative, the First Responder Training portal, that will be the primary location for information and resources serving the first responder community in support of the DHS strategic goal of improving the nation's ability to prevent, prepare, mitigate, respond to, and recover from emergency situations and events. The portal will create a functional tool to support the development and delivery of efficient, effective and consistent first responder training. Registered under the domain name of firstrespondertraining.gov, the website will provide a single, authoritative link for the first responder community and will include collaboration tools and information on training, grants, equipment, and standards.

This portal will complement FEMA/U.S. Fire Administration's (USFA) existing on-line training portals, the Emergency Management Institute's Independent Study website, and the USFA National Emergency Training Center (NETC) Virtual Campus, which together offer more than 60 courses for emergency personnel and has registered more than 350,000 course completions already this fiscal year. The NETC Virtual Campus courses are intended for Federal, state, and local officials including emergency management personnel, fire service personnel, police, public works, health officials and first responders, and also DHS personnel, and the general public.

The ODP First Responder Training portal and FEMA's on-line training facilities will provide consistent delivery of training to large audiences and will be used as a delivery mechanism by our partners to continue to enhance the capacity of the emergency responder community. Additionally, this web-based training will: accommodate students with disabilities by use of assistive technologies; be designed to support small group work and collaboration; provide multi-purposed training and resources; have the capability to restrict access to only authorized users; offer students the opportunity to remediate materials until proficient or "opt out" of content they have already mastered; and be linked through other initiatives currently underway to track user activity and accurately provide student transcripts.

The framework and inter-workings of the overall system are nearing completion. A pilot test, testing functionality and usability for internal users/developers (training partners) and external users (students from the first responder communities), will begin in June 2005. Results from the pilot test will be used to make improvements to the system and to determine the effectiveness of the technology in support of ODP's National Training Program.

Prior to the development of the First Responder Training portal, ODP developed a Training Course Catalog, as well as comprehensive guidelines associated with attending ODP-sponsored training courses. This information is available to the Nation's first responder community through a number of different means, including ODP's publicly-available website (http://www.ojp.usdoj.gov/odp) as well as through routine interaction with ODP's State Preparedness Officers and the nation's first responder community. As New Mexico Tech develops training courses at Playas Training Center, ODP will make this information available through its various outreach mechanisms, including the First Responder Training portal.

New Mexico Capabilities—Dirty Bomb Training

Question. New Mexico Tech has also joined with New Mexico State University ("NMSU") to propose an expansion of the anti-terrorism training program for first

responders. This expansion would include a course about radiological dispersal devices (also known as dirty bombs).

I believe this proposal has merit because the aftermath of a dirty bomb attack is one of our gravest anticipated terrorist attacks, and our first responders need appropriate training to respond to such a threat. New Mexico Tech and NMSU's Carlsbad Environmental Monitoring and Research Center have the scientific expertise, radiological handling capabilities, radioactive material license, and trained staff to address both the scientific and training aspects of dirty bombs, and collaboration between these universities and New Mexico's national nuclear weapons labs could provide ideal training first responders to counter dirty bomb risks.

What dirty bomb training do Federal first responders currently receive?

Answer. FEMA/USFA's Emergency Management Institute (EMI), as well as the National Fire Academy, offers a full range of courses that prepare state, local, and tribal emergency personnel to deal with the aftermath of all types of events involving radiological materials. EMI courses such as "Radiological Emergency Response Operations" and "Advanced Radiological Incident Operations" and the NFA's Command and Control of Emergency Incidents provide specific instruction in how to prepare for such events.

Although there is no specific course dedicated to radiological dispersal devices, several courses delivered by members of the National Domestic Preparedness Consortium (NDPC) cover radiological dispersal devices in their course curriculum. The extent to which radiological dispersal devices are covered in the various courses ranges from a five minute overview to a detailed 2.5 hour block of instruction. States, territories, and urban areas may use SLGCP-certified training to enhance the capabilities of State and local emergency preparedness and response personnel as it adheres to the State's Homeland Security Strategy. The target audience for SLGCP-certified training courses includes State and local emergency preparedness, prevention and response personnel; emergency managers; and public/elected officials within the following disciplines: fire service, law enforcement, emergency management, emergency medical services, hazardous materials, public works, public health, health care, public safety communications, governmental administrative, cyber security, and private security providers.

Question. Could New Mexico Tech's training facility in Playas, New Mexico be the ideal place to base such training?

Answer. As you are aware, ODP has funded the New Mexico Institute of Mining and Technology since fiscal year 1998 as part of the National Domestic Preparedness Consortium. As part of the Consortium, the New Mexico Institute for Mining and Technology supports ODP's mission of assisting State and local governments plan and prepare for incidents of domestic terrorism by providing critical training to the nation's first responders. ODP periodically reviews its training requirements and builds on the strengths of its training partners. Currently, nuclear and radiological training primarily falls under the Department of Energy's Nevada Test Site (NTS). However, ODP will review any unique capabilities the Playas Training Center may offer.

RESEARCH AND TECHNOLOGY—GENERALLY

Question. The Department of Homeland Security has used many different resources to implement innovative protective measures across the country. We have improved security nationwide through the Department's Science and Technology Directorate, the Advanced Research Projects Agency, Centers of Excellency, and similar divisions and initiatives.

The Department's leadership in developing innovative tools and technologies to protect our Nation is one of the most important roles the Department plays. However, with so many groups working on developing new technologies, it may prove difficult to select the best technology available.

How does DHS intend to most effectively integrate and leverage existing efforts and capabilities to ensure that the best technologies available are utilized?

Answer. Last year, the S&T Directorate developed and documented a robust RDT&E process. The goal of the RDT&E process is to provide a clearly defined, repeatable method for assessing needs and risk, planning, allocating resources and executing programs to produce high-impact, cost-effective and critically needed homeland security technology solutions.

The S&T Directorate's RDT&E process uses a risked-based approach to planning and identifies critical capability gaps before attempting to identify or develop technology solutions. In developing solutions, the process engages the end-user throughout requirements definition, development, testing and transition. The process considers the product life cycle from the outset, including planning and budgeting for

production, deployment, operations and support. It is this process which allows us to prioritize both within and across fields.

Integration of existing efforts and capabilities occurs in several key areas. For example, the S&T Directorate collaborates with academia through the Centers of Excellence program and its associated Integrated Network of Centers, which is establishing a national network of affiliated universities. Additionally, the S&T Directorate has a sizeable number of interactions and programs with individual universities on specific research topics and needs.

The S&T Directorate also maximizes and leverages the existing capability base of the national laboratory complex. The Directorate engages all the national laboratories on a case-by-case basis, to tap into unique technical expertise that is critical to accomplishing portfolio objectives and goals. The Directorate also relies on national laboratory technical experts as needed throughout the RDT&E processes based on their years of experience applying technologies and processes to field applications. This technical and practical expertise is used to accelerate spiral development of technologies for transitioning capabilities to operational end-users.

The S&T Directorate solicits proposal from industry and uses a full range of contracting vehicles and its authority under the Homeland Security Act to engage businesses (large and small), Federally funded research and development centers, universities, and other entities in development of advanced technologies for homeland security. The contracted research and development work now underway is the S&T Directorate's main form of collaboration with industry and academia.

Question. Under your leadership, how will the Science and Technology Directorate collaborate with academia, industry and our national labs?

Answer. The S&T Directorate collaborates with academia through the Centers of Excellence program and its associated Integrated Network of Centers, which is establishing a national network of affiliated universities. Additionally, the S&T Directorate has a sizeable number of interactions and programs with individual universities on specific research topics and needs.

The S&T Directorate solicits proposals from industry and uses a full range of contracting vehicles and its authority under the Homeland Security Act to engage businesses (large and small), Federally funded research and development centers, universities, and other entities in development of advanced technologies for homeland security. The contracted research and development work now underway is the S&T Directorate's main form of collaboration with industry and academia.

The S&T Directorate maximizes and leverages the existing capability base of the national laboratory complex. The Directorate engages all the national laboratories on a case-by-case basis, to tap into unique technical expertise that is critical to accomplishing portfolio objectives and goals. The Directorate also relies on national laboratory technical experts as needed throughout the RDT&E processes based on their years of experience applying technologies and processes to field applications. This technical and practical expertise is used to accelerate spiral development of technologies for transitioning capabilities to operational end-users.

The S&T Directorate engages all the national laboratories on a case-by-case basis, to tap into unique technical expertise that is critical to accomplishing portfolio objectives and goals. The Directorate also relies on national laboratory technical experts as needed throughout the RDT&E processes based on their years of experience applying technologies and processes to field applications. This technical and practical expertise is used to accelerate spiral development of technologies for transitioning capabilities to operational end-users.

For example, the Countermeasures Test Beds (CMTB) program operates in close partnership with a number of Federal and national laboratories to execute its mission of testing and evaluating all threat countermeasures and systems. The following national labs participate in all CMTB Operational Testing and Evaluation (OT&E) efforts and enable deployments in response to heightened alert conditions as necessary. Multi-lab teams are encouraged to ensure objectivity and a healthy interchange of ideas.

As another example, the Office of Interoperability and Compatibility (OIC) is currently leveraging the resources of Eastern Kentucky University in developing effective test methodologies for equipment and to provide technical assistance to States and localities under the SAFECOM Program. At the same time, OIC has enlisted a consortium of well over one hundred universities and colleges to support the annual conference on Technologies for Public Safety in Critical Incident Response, jointly sponsored by DHS and the DOJ. Industry associations participate in SAFECOM Program activities, especially in standards development efforts. OIC has established a monthly vendor process which allows for constant communication and collaboration with our industry partners. Additionally, OIC/SAFECOM will be conducting an industry summit in late fall to allow for ever greater collaboration.

Additionally, the BioSecurity program currently works closely with academia, industry and the national labs to fulfill its national mission.

Question. How will you allocate funding to national laboratories, universities, and industry in a competitive and transparent manner?

Answer. The S&T Directorate supports seeking the best sources to accomplish DHS RDT&E goals through full and open competition.

Individual national laboratories have recognized expertise in specific technical fields built up from years of experience in national defense technology development. Recognizing those areas of expertise, integrated technical programs have been formed from multiple laboratories to solve problem sets related to their expertise. The laboratories assist in leading the formation of the technical teams addressing specific problem sets. The S&T Directorate uses a performance based approach to ensuring quality programs. As such, annual external reviews are conducted with subject-matter experts and end-user reviewers to evaluate the performance and outcomes of individual programs. Results from these reviews are documented and used to inform decisions on the next fiscal year's program execution plans.

All funds allocated by University Programs to universities and individuals at universities are the product of a highly competitive merit-based selection process. A large number of subject matter experts from government, industry and academia use well-established and documented peer review selection procedures in making funding recommendations.

All S&T Directorate Broad Agency Announcements and Small Business Innovation Research solicitations are public and competitive. All are published on the official Federal Government procurement website (and simultaneously on the S&T Directorate's HSARPA websites) and each contains explicit instructions on how to submit white papers and proposals. The criteria by which these submissions will be evaluated for technical merit are published in each solicitation. The source selection plan which guides the panel of experts who evaluate the submissions is approved at the same time the solicitation is published and records of their final decisions are retained. Selections for funding are typically made on technical merit, relevance to DHS mission, available funding, and programmatic considerations by a source selection authority.

Also, the S&T Directorate works to ensure all of its program offices allocate funding to national and Federal laboratories, universities, and industry where appropriate, following the competitive guidelines outlined in the Federal Acquisition Requirements. The S&T Directorate continually monitors all program aspects to determine best value and cost effectiveness. As the S&T Directorate works to mature and transition mature technologies to the user community, a competitive process is used.

RESEARCH AND TECHNOLOGY—NISAC

Question. The National Infrastructure Simulation and Analysis Center, or NISAC, is funded by DHS to evaluate the effects of disruptions to America's infrastructure, and much of NISAC's work is done by New Mexico's two National Laboratories: Sandia and Los Alamos.

I strongly believe in NISAC's efforts and capabilities, but I do not believe the program is being used by the entire Department of Homeland Security to its full extent.

What are your plans to coordinate the Department's Directorates so NISAC is utilized by the entire Department?

Answer. The Department's National Infrastructure Simulation and Analysis Center (NISAC) is a program in the DHS IAIP Directorate. Since its inception, NISAC has had the mission to provide comprehensive modeling and simulation capabilities for the analysis of critical infrastructures, their interdependencies and complexities, and the consequences of disturbances. This mission and NISAC's expertise directly support the modeling, simulation, and analysis initiatives of DHS. For fiscal year 2005, IAIP will continue to expand NISAC's operational development of a suite of infrastructure modeling, simulation and analytic capabilities with an emphasis on interdependencies and consequences of infrastructure disruptions for the Nation as a whole.

At present, IAIP is coordinating ongoing NISAC work with the S&T Directorate, the Coast Guard, FEMA, BTS, and TSA, as well as with the Departments of Transportation and Energy, on multiple projects that concern the nation's infrastructure. The NISAC program office will continue its efforts to broaden the awareness of the NISAC program throughout DHS to ensure this national resource is properly tasked with the most urgent and complex problems concerning infrastructure dependencies and interdependencies. IAIP will continue to fully utilize, and if warranted expand, the existing capabilities of NISAC with IAIP acting as the central coordinator for

NISAC efforts in keeping with IAIP's national charter of coordinating and leading efforts for the understanding and protection of the nation's infrastructure. Moreover, as the Department's ability to execute risk assessment continues to mature, NISAC will become more and more integrated into the full range of Federal risk management programs.

Question. How will you work with the Director of National Intelligence to make NISAC's capabilities available to the intelligence community through a formal relationship, as required by last year's intelligence reform bill?

Answer. IAIP is continually improving the integration between the organizations that develop the three components of our Strategic Risk Analysis; which are consequence, vulnerability and threat or attractiveness. A prime example of this effort is ensuring that the intelligence component of DHS, the Office of Information Analysis, currently in IAIP, is aware of NISAC's capabilities and, as a byproduct, the resident expertise at the national laboratories. As the NISAC products are more fully developed and matured, this integration will increase.

As a continuation of this integration, we will engage with the Director of National Intelligence to make him aware of a variety of efforts the Department has underway that will benefit from his efforts, NISAC included. We will seek a formal relationship for information and capability sharing as warranted, between non-DHS elements of the intelligence community and the Department, including the NISAC.

Question. What do you need from Congress to fully implement NISAC's capabilities?

Answer. Congress's continued support for all of the Department's programs that seek to reduce the risk of terrorism to the Nation are greatly appreciated. All of these programs are essential, including the Department's National Infrastructure Simulation and Analysis Center.

RESEARCH AND TECHNOLOGY—DOMESTIC NUCLEAR DETECTION OFFICE (DNDO)

Question. The Department has a new office tasked with deploying radiation detection technologies and systems designed to detect attempts to smuggle nuclear materials or weapons into the United States. As such, the Domestic Nuclear Detention Office, is likely to play a critical role in testing and evaluating current and next generation technologies to assure that DHS agencies have the most effective and accurate tools.

How does DNDO intend to balance the needs between rapidly deploying detection systems and developing technologies that can best fulfill its mission?

Answer. The DNDO will include, as part of its staff, an Office of Systems Engineering, which will be dedicated to development of the global systems architecture, as well as a comprehensive systems engineering capability. This office will be tasked with providing quantifiable analysis of issues such as this and providing cost-benefit analysis, when appropriate, to determine the relative advantages gained by deploying current technologies or developing additional capabilities.

Additionally, beyond the DNDO office structure, the DNDO will also utilize the Department's robust, two-tiered validation process for large-scale programs, consisting of a Joint Requirements Council and an Investment Review Board, which have final approval to authorize deployment or development programs.

Question. How do you plan to develop and support the nuclear facilities and infrastructure needed to test and evaluate evolving technologies, missions, and operational concepts?

Answer. The DNDO will continue to proceed with the design and construction of the Radiological and Nuclear Countermeasures Test and Evaluation Complex (RadNucCTEC) at the Nevada Test Site. The construction of this facility, begun within the DHS S&T Radiological and Nuclear Countermeasures portfolio, will bridge the gap between "bench-top testing" performed by developers and operational field testing conducted during pilot deployments, providing the unique capability to test systems in a near real-world environment against actual special nuclear materials in authentic configurations. Construction is expected to begin in June 2005 and be completed by the end of fiscal year 2006.

Additionally, DNDO will continue to utilize the DHS S&T Countermeasures Test Bed (CMTB) for operational testing and evaluation. CMTB will provide a critical, objective testing environment to evaluate technologies and concepts of operation for nuclear and radiological detection in key operational venues.

Question. With the creation of DNDO, will the efforts to prevent and respond to radiological dispersion devices be retained in the Science and Technology Directorate, moved into DNDO, or shared between these two DHS divisions?

Answer. Many experts consider a nuclear attack to be less likely than the release of a radiological dispersion device (RDD). However, a nuclear attack would be many

times more devastating than one employing an RDD, both in terms of economic impact and casualties. While the primary focus of DNDO is, therefore, to develop and acquire systems and capabilities for the detection of special nuclear materials (SNM) and nuclear devices, most nuclear threat detection systems will also detect radiological threats, because of the similarity in nature of radioactive signatures of special nuclear materials nuclear devices and radiological materials usable in an RDD.

As such, the division of responsibilities for prevention and response for RDDs between DNDO and the S&T Directorate is the same as that for nuclear devices or materials. DNDO will be responsible for the development of the detection architecture, as well as the systems to be deployed, for the prevention of an attack. Additionally, DNDO will be responsible for the development of training and response protocols in the event of an alarm. However, DNDO will not be responsible for the development of incident management or decontamination technologies; these programs will remain in the S&T Directorate.

Question. What role will national weapons labs play in DNDO?

Answer. DNDO will continue to work with the Office of National Laboratories in the S&T Directorate to make sure that work is properly coordinated and that all of the national laboratories, including the weapons labs, receive clear guidance and direction on efforts they conduct with DNDO or the S&T Directorate.

DNDO recognizes that the national weapons laboratories have long been one of this nation's preeminent sources of critical nuclear expertise. That expertise, along with the expertise found in academia and industry, will be vital to responding to the threat posed by nuclear and radiological weapons or materials and in developing transformational capabilities to significantly enhance the U.S. capability to protect against this threat.

QUESTIONS SUBMITTED BY SENATOR ROBERT C. BYRD

DRUG TRAFFICKING

Question. The President has said, "trafficking in drugs finances the work of terrorists, sustaining terrorists and that terrorists use drug profits." Given the President's view, I am surprised that he has included almost no initiatives in your budget to disrupt the drug trade. Why?

Answer. The fiscal year 2006 President's Budget includes $3.455 billion that affects or may affect the counternarcotics activities of the Department or any of its subdivisions, or that affects the ability of the Department or any subdivision of the Department to meet its responsibility to stop the entry of illegal drugs into the United States.

Within that $3.455 billion total, approximately $2.937 billion has been identified as National Drug Control Budget Funds—funds for those Department programs and initiatives that directly support Priority III of the President's National Drug Control Strategy (Disrupting the Market: Attacking the Economic Basis of the Drug Trade). This funding will provide the Department with resources to strengthen and focus its illegal drug market disruption efforts while, at the same time, dedicating new resources for emerging threats. In addition to these funds, approximately $480.5 million has been identified as other potential expenditures that also may affect the counternarcotics activities of the Department.

These funds support counternarcotics programs and counternarcotics-related activities that can build on the Department's many accomplishments towards stopping the entry of illegal drugs into the United States.

LOBBYING RULES

Question. On November 23, the Office of Government Ethics, in response to a Department of Homeland Security (DHS) request, relaxed lobbying prohibitions for former "senior employees" of the Department. Up until November 23 of this year, any former "senior employee" of DHS was barred from lobbying any individual or office in DHS for 1 year. A senior employee is any individual whose rate of basic pay is equal or greater than 86.5 percent of the rate for level II of the Executive Schedule. The 2004 salary for an Executive Level II employee is $158,100, 86.5 percent of which is $136,756.

The revised rule by the Office of Government Ethics designates seven distinct and separate components in DHS for purposes of 18 U.S.C. 207(c), which covers conflict of interest restrictions for senior Federal officials in post-employment. The components designated are: Transportation Security Administration (TSA); Coast Guard; Secret Service; Federal Law Enforcement Training Center (FLETC); Science &

Technology (S&T) Directorate; Information, Analysis & Infrastructure Protection (IAIP) Directorate; and Emergency Preparedness & Response (EP&R).

By designating seven distinct and separate components in DHS, any former official who worked in one of those seven components is now permitted to immediately lobby anywhere in DHS except for the component for which they were employed. It also allows senior officials who worked for DHS, but not in one of the seven designated components, to immediately lobby anyone in those components designated as distinct and separate. For instance, a senior employee who worked in the Office of the Secretary for Tom Ridge can immediately lobby any of the DHS organizations cited above. Those seven components alone comprise over $19 billion and nearly 60 percent of the Department's funding.

Why did DHS request this change to the lobbying rules?

Answer. The recommendations were made to appropriately tailor the application of the 1-year cooling-off restriction to the circumstances existing within the newly created Department of Homeland Security. Section 207 of title 18 of the United States Code is not intended as a blanket bar to former employees from dealing with the Government after separation. Rather, it represents a carefully crafted balance between preventing improper peddling of influence in the government by former government officials on the one hand, and permitting the continued availability to the government of the experience and training of former government officials. In a dynamic, forwarding leaning agency such as DHS, with a mission to protect the homeland, it is essential that the agency attract top notch people who are facile and knowledgeable about innovative technology. The DHS mission requires that these leaders in the fields populate the whole of DHS Headquarters and its components.

The statute is composite of a series of very fact specific prohibitions based on conclusions of improper over-reaching as determined though the lens of that balancing. Congress recognized the potential subsection 207(c) has to unduly restrict appropriate post-Government-service interaction by former employees with the government by carving out exceptions to it, i.e., subsection 207(c)(2)(B)(in the cases of special government employees), subsection 207(c)(2)(C)(in cases of difficult-to-fill positions), subsection 207(h)(in cases of elements of an agency where there exists "no potential for use of undue influence or unfair advantage based on past Government service"), and subsection 207(j)(Exceptions).

The recommendations that DHS made to the Director, Office of Government Ethics, in December 2003, were based on the following:

—OGE criteria for making such recommendations;

—how the Department was structured and operating;

—how the legacy agencies had treated the organizational elements previously; and

—how subsection 207(c) is applied generally through the Executive Branch.

Several features of the Department were clear for the purposes of these recommendations. United States Secret Service, the United State Coast Guard, the Transportation Security Agency, and the Federal Law Enforcement Training Center were focused on discrete independent missions of the Department, most statutorily so, and had extensive independent administrative structures. The three directorates, Science and Technology, Information Analysis and Infrastructure Protection, and Emergency Preparedness and Response, posed a more nuanced picture, but presented the same distinct, self-contained mission focuses.

Equally clear in the opposite direction was that the significance of the missions entrusted to the Border and Transportation Security Directorate and its subordinate elements and the extensive vertical and horizontal interaction between them made them so inter-related and inter-dependent as to foreclose designating them as separate.

Given those conclusions and comparing how other agencies treated their components, we recommended the designation of those seven components as separate for the purposes of the 1-year cooling-off period.

Question. How is this change beneficial to the Department, the U.S. taxpayers, and our national security?

Answer. The Department's exercise of this statute greatly enhances national security, benefits the taxpayers of the United States, and is invaluable in the accomplishment of the Department's mission. Detection of threats by passage of people and cargo into the United States by air, sea, or land is dependent upon innovative human and technological systems that are used by components throughout the Department. These systems were developed by career and non-career Federal employees working as a team. The career employees contribute their expertise and experience in government operations and the non-careerist often contribute their expertise and experience in technology developed in the private sector. It is a proven successful synergy, not quite perfect, but the best in the world.

Our nation's security and the taxpayer will be the ultimate losers if the country's professionals and leaders are kept from joining Federal agencies initially or, upon return to the private sector, are precluded from bringing their skills and experience to bear on these important issues because of a failure to appropriately tailor the post-Government-service restriction. The departing leaders take with them an understanding of the threat, what is needed to combat the threat, and how the Department is working to counter the threat. The threat is not stagnant, and it is counterproductive to overly restrict the work of those who are among the most able to ensure close cooperation and understanding between the Federal and non Federal entities to make our country safe.

We believe that the combination of the relaxation of the restriction imposed by section 207(c) granted by the designation of separate components and the existence of the additional restriction applicable to very senior personnel, the inapplicability of separate component designation to our former employees who were paid pursuant to the Executive Schedule, and the application of subsection 207(d), we have achieved the balance that was desired by the drafters of section 207. Of course, we must certify annually to the Director, United States Office of Government Ethics, that our designations remain appropriate.

DHS HEADQUARTERS

Question. In addition to the $25 million GSA is requesting to locate CG headquarters at St. Elizabeth's campus in Anacostia, there is a $13 million request for "St. Elizabeths West Campus Infrastructure". The West Campus alone has 182 acres and includes 61 buildings. The justification says "the site is aptly suited to provide a high security campus for Federal agencies."

What are the Department's plans for the St. Elizabeth site?

Answer. The Department's plans for the St. Elizabeth site are to ensure that the Coast Guard headquarters is properly planned and executed to provide additional expansion capability should the need arise for additional occupancy.

Question. How are these plans related to the current efforts to outfit the Nebraska Avenue complex?

Answer. The requirements for adjacency and mission needs being established at the NAC would be utilized should the opportunity for expansion be available at the St. Elizabeth site.

AVOIDING FUTURE FUND LAPSES

Question. Why did the Department Management account allow $9.3 million to lapse at the end of fiscal year 2004 and what specific systems have been put in place to make sure that this does not happen again?

Answer. The Department did not intentionally allow funding to lapse in fiscal year 2004. The fiscal year 2004 unobligated balance for the Departmental Management account was due primarily to slower than anticipated hiring, resulting in personnel lapse. In fiscal year 2004, the infrastructure and organization to manage budget execution for Departmental Management was not fully developed. The transition to a new accounting system and financial services provider in fiscal year 2004 created additional challenges and complexities, along with a learning curve, which made it difficult for financial managers to track spending during the year. In fiscal year 2005, we now have more staff and contractors onboard to perform budget execution activities for the Departmental Management account and can provide more useful data to managers to manage their budgets more efficiently and effectively.

Question. Do you plan to seek authority to reprogram the lapsed funds?

Answer. The Department submitted a request as part of the ICE reprogramming package to use the lapse authority under Section 504 to transfer $2.8 million from fiscal year 2004 lapsed funding from the Departmental Management account to ICE for its funding shortfall. This reprogramming request was overtaken by the fiscal year 2005 Emergency Supplemental Appropriations Act for Defense, the Global War on Terrorism and Tsunami Relief, H.R. 1268 recent Supplemental that was passed that rescinded a total of $3.8 million from Departmental Management that was proposed in the ICE programming, including the $2.8 million from the fiscal year 2004 lapsed monies.

CLASSIFIED VS. SENSITIVE INFORMATION

Question. Late last year there were articles in various papers, including The Washington Post, regarding how the Department handles information it determines to be "sensitive" versus actually "classified" material. It has required Federal Government employees, including congressional staff with "Top Secret" clearances, to sign confidentiality documents demanding that these previously cleared personnel

not reveal information that, technically, is not "classified". Most recently, on December 13, 2004, the Heritage Foundation released a report entitled, "DHS 2.0: Rethinking the Department of Homeland Security". One of its conclusions calls for the Department to develop a "consistent policy and legislation that encourages the sharing of unclassified but security-relevant information between the private sector and the government." This might also include the dropping or reconsideration of the documents security classification known as "Sensitive Security Information."

What public law created the classification known as "Sensitive Security Information"?

Answer. Following the terrorist attacks on the United States on September 11, 2001, Congress passed the Aviation and Transportation Security Act (ATSA), Public Law 107–71 (November 19, 2001), which established the Transportation Security Administration (TSA). ATSA transferred the responsibility for civil aviation security from the Federal Aviation Administration (FAA) to TSA. Among the statutory authorities previously administered by FAA that ATSA transferred to TSA's purview was the authority in 49 U.S.C. § 40119, governing the protection of certain information related to transportation security.

On February 22, 2002, TSA published a final rule transferring the bulk of FAA's aviation security regulations to TSA, including FAA's SSI regulation, which now is codified at 49 CFR Part 1520.

In addition, on November 25, 2002, the President signed into law the Homeland Security Act of 2002 (HSA), Public Law 107–296, which transferred TSA to the newly established DHS. In connection with this transfer, the HSA transferred TSA's SSI authority under 49 U.S.C. § 40119 to 49 U.S.C. § 114(s), and amended section 40119 to vest similar SSI authority in the Secretary of DOT. [See Section 1601 of the HSA.]

It should also be noted that Sensitive Security Information (SSI) is not a classification, and information designated as SSI is not considered as classified national security information.

Question. Is the Department, as part of your overall review of its operations, actively considering the Heritage Foundation recommendations on protecting sensitive information? If not, why not?

Answer. Yes. The Department has carefully reviewed a number of recommendations and proposals regarding information sharing, and it is working to develop and establish a consistent prudent strategy on the subject. The guiding principle must balance the need to share information with appropriate individuals, while still protecting the sensitive nature of the underlying information.

CONTRACTING OUT REPORT

Question. The fiscal year 2004 Appropriation Omnibus (H.R. 2673) Division F—Departments of Transportation and Treasury, and Independent Agencies, Title VI Section 647(b), contained the following reporting requirement: "Not later than 120 days following the enactment of this Act and not later than December 31 of each year thereafter, the head of each executive agency shall submit to Congress a report on the competitive sourcing activities on the list required under the Federal Activities Inventory Reform Act of 1998 (Public Law 105–270; 31 U.S.C. 501 note) that were performed for such executive agency during the previous fiscal year by Federal Government sources.

The Committee received this report on February 3, 2005. The report states that two public-private competitions, which were started in September of 2004, are scheduled for completion in fiscal year 2005. In addition, the report states that additional competitions are scheduled to be held in fiscal year 2005 which will involve up to 1,397 FTE.

Please provide the Committee an updated report containing the most recent fiscal year 2005 information as well as any plans for public-private competitions in fiscal year 2006.

Answer. In fiscal year 2005, DHS is currently completing the competitions involving 357 FTE. This includes competitions being conducted at the U.S. Coast Guard (USCG), CBP, and the FLETC. DHS is currently reviewing proposals for the completion of competitions in fiscal year 2006.

The DHS's annual Reports to Congress, as required by Section 647(b) of Division F of the Consolidated Appropriations Act, fiscal year 2004 (Public Law 108–199) are available on our web-site at: http://www.dhs.gov/dhspublic/display?theme=37&content=3933

Question. For fiscal year 2004 (actual), fiscal year 2005 (estimate), and fiscal year 2006 (request), how many positions in the Department (broken down by agency) were competed and how much did the competitions cost.

Answer. In fiscal year 2004, DHS completed three public-private competitions, in accordance with the OMB Circular A–76, involving 144 FTE at the USCG. Two DHS competitions that were scheduled for completion in fiscal year 2004 were cancelled in fiscal year 2004:

—The USCG's competition of its military travel support function (36 FTE) was cancelled due to the development of E-Travel technologies that will obviate the current approach to this service requirement;

—The Citizenship and Immigration Service (CIS) competition of its Immigration Information Officer (IIO) function (1,350 FTE) was cancelled to give more time and resources to the elimination of immigration service backlogs and, as a matter of law. DHS announced two ICE competitions for completion in fiscal year 2005. These competitions involved 97 FTE, but were also cancelled due to funding shortages.

Savings generated by the three completed fiscal year 2004 USCG competitions are estimated at $12.3 million over a 5 year period. All three competitions were retained in-house. The incremental cost of conducting these USCG studies is estimated at $1.3 million and reflects the costs incurred in gearing up the competition program in the USCG. In addition, four FTE are associated with DHS' fiscal year 2004 fixed costs—spread across the agency—and are estimated at $450,000 per year. The DHS fixed program cost estimate includes dedicated resources to provide central policy, planning, and implementation oversight, yet excludes annual FAIR Act inventory costs. The estimated one-time DHS cost of conducting the fiscal year 2005 competitions involving 356 FTE is $1.9 million, with expected annual savings in excess of $5 million. The estimated one-time cost of conducting the fiscal year 2006 competitions is not known, as we have not yet finalized those plans.

Question. How many positions were subsequently contracted out as a result of the competition?

Answer. While there have been significant efficiency and quality of service gains on the part of the government as a result of engaging in the fiscal year 2004 and fiscal year 2005 competitions, to date no positions have been converted to contract performance.

DETAILEES TO THE WHITE HOUSE

Question. How many DHS employees (including the component agencies) are currently detailed to the White House (including all Executive Office of the President agencies)? Provide the committee a list containing the originating agency; the office they are detailed to; salary grade/step; length of detail (including beginning and end dates); purpose of the detail; and indicate if the agency is reimbursed.

Answer.

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
NSC	DHS/IAIP	GS 12–01 ($62,886)	3/20/2004	12/30/2005	Communications and Media Relations. Was part of GSA technology office that was absorbed by DHS in early 2003.	N
NSC	DHS/USCG	MILITARY	6/14/2004	6/13/2006	White House Situation Room Duty Officer	N
NSC	DHS/USCG	MILITARY	6/21/2004	6/20/2005	Counternarcotics	N
NSC	DHS/USCG	MILITARY	10/6/2003	6/10/2005	White House Situation Room Duty Officer	N
NSC	USSS	GS 14–02 ($91,315)	4/18/2005	4/17/2006	Combating Terrorism	N
ONDCP	U.S. Coast Guard	MILITARY	7/15/2004	7/15/2005	Office of Supply Reduction	N
WHO	DHS/TSA	K–00 ($111,038)	5/21/2004	9/30/2005	Support the WHO mission	N
WHO	DHS		7/24/2004	1/19/2006	Support the WHO mission	N
WHO	DHS/USSS	GS 14–04 ($97,206)	6/22/2004	9/30/2005	Support the WHO mission	N
WHO	U.S. Coast Guard	MILITARY	9/22/2004	1/19/2006	Support the WHO mission	N
OVP	U.S. Coast Guard	MILITARY	5/17/2005	7/15/2007	Military Aide to the Vice President	N
OVP	U.S. Coast Guard	MILITARY	6/16/2003	7/1/2005	Special Advisor, Homeland Security	N
OVP	U.S. Coast Guard	MILITARY	4/22/2003	6/29/2005	Military Aide to the Vice President	N

DETAILEES TO THE DEPARTMENT

Question. How many employees of DHS component agencies are currently detailed to the Department? Provide the committee a list containing the originating agency; the office they are detailed to; salary grade/step; length of detail (including beginning and end dates); purpose of the detail; and indicate if this agency is reimbursed.

Answer. The table below provides the requested data, which is a snapshot of detailees on-board as of March 31, 2005. This data submission was done in April 2005 and projected end dates that could have ended by the time this report was submitted.

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
USM/CIO	BTS	$117,809	6/1/2004	6/1/2005	DHS Infrastructure trans support	N
BTS	CBP	$149,200	7/27/2004	7/27/2005	BTS	N
BTS	CBP	$121,274	9/2/2003	9/2/2005	Cargo/Trade Policy	N
BTS	CBP	$117,809	9/7/2004	9/6/2005	Border Patrol Liaison	N
BTS	CBP	$117,809	2/23/2003	(1)	Counternarcotics Projects	N
BTS	CBP	$100,152	7/27/2004	7/27/2005	CIO Assistant	N
BTS	CBP	$94,260	12/6/2004	12/7/2005	Agency Liaison Officer	N
FLETC	CBP	$81,638	10/7/2002	(1)	Instructor	N
FLETC	CBP	$81,638	5/15/1995	(1)	Instructor	N
FLETC	CBP	$81,638	9/2/2003	9/2/2006	Instructor	N
FLETC	CBP	$68,651	5/1/2004	5/1/2007	Instructor	N
FLETC	CBP	$81,638	2/18/1998		Instructor	N
FLETC	CBP	$68,651	10/1/2002	(1)	Instructor	N
FLETC	CBP	$81,638	2/16/1993		Instructor	N
FLETC	CBP	$68,651	5/16/2004	5/16/2007	Instructor	N
FLETC	CBP	$81,638	11/19/2001	(1)	Instructor	N
FLETC	CBP	$81,638	8/13/1998		Instructor	N
FLETC	CBP	$68,651	10/27/2003	10/27/2008	Instructor	N
FLETC	CBP	$68,651	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	11/6/1990		Instructor	N
FLETC	CBP	$81,638	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	9/25/2000		Instructor	N
FLETC	CBP	$81,638	3/22/2004	3/22/2007	Instructor	N
FLETC	CBP	$81,638	12/23/2000		Instructor	N
FLETC	CBP	$81,638	6/1/1998	(1)	Instructor	N
FLETC	CBP	$81,638	9/29/1997		Instructor	N
FLETC	CBP	$81,638	1/25/1993	(1)	Instructor	N
FLETC	CBP	$68,651	2/24/2004	(1)	Instructor	N
FLETC	CBP	$81,638	7/30/1997	(1)	Instructor	N
FLETC	CBP	$81,638	8/27/2001	8/27/2006	Instructor	N
FLETC	CBP	$57,280	4/15/2002	4/15/2007	Instructor	N
FLETC	CBP	$68,651	7/14/2003	(1)	Instructor	N
IAIP	CBP	$131,671	10/1/2004	(1)	HSOC	N
IAIP	CBP	$91,315	1/10/2005	7/10/2005	Terrorist Screening Ctr	N
IAIP	CBP	$69,173	11/28/2004	5/17/2005	HSOC	N
IAIP	CBP	$73,364	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$75,460	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$62,886	11/17/2003	5/31/2005	Support to IAIP Terrorist Screening Center	N

IAIP	CBP	$77,274	9/12/2003	(1)	HSOC	N
IAIP	CBP	$69,173	12/12/2004	6/14/2005	HSOC	N
IAIP	CBP	$77,274	3/20/2005	3/20/2006	COMSEC	N
ICE	CBP	$52,468	3/21/2005	3/21/2006	Visa Security Program	N
ICE	CBP	$124,274	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$43,724	11/1/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$61,213	10/23/2004	3/31/2005	Visa Security Unit	N
ICE	CBP	$91,315	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$97,213	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$91,315	9/20/2004	6/1/2005	Visa Security Unit	N
ICE	CBP	$68,209	11/17/2004	4/29/2005	Visa Security Unit	N
ICE	CBP	$117,809	12/7/2004	TBA	Assist ICE HR Officer	N
OIA	CBP	$62,886	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$57,715	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$64,981	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OPA	CBP	$128,205	1/26/2004	(1)	Public Affairs	N
USCG	CBP	$77,274	8/4/2003	(1)	Support to USCG	N
USM/CFO	CBP	$114,344	1/1/2004	(1)	OCFO	N
USM/CFO	CBP	$103,947	10/20/2003	10/19/2005	Support eMerge project	N
USM/CFO	CBP	$106,044	10/1/2003	10/1/2005	Support eMerge project	N
USM/CHCO	CBP	$100,152	4/28/2004	(1)	New HR system: communications team	N
USM/CIO	CBP	$100,152	5/1/2004	5/1/2005	Infrastructure Transformation Office	N
USM/CIO	CBP	$117,344	11/10/2003	6/30/2005	Program manager—HSDN	N
USM/CIO	CBP	$149,200	10/6/2004	7/31/2005	CIO	N
USM/CIO	CBP	$43,365	11/9/2004	9/15/2005	CIO support	N
S&T	CG	$84,751	6/30/2004	6/30/2007	Providing technical expertise to S&T	Y
USM/CIO	CIS	$89,736	3/1/2003	(1)	Support DHS' Infrastructure Transformation Office	N
USM/CIO	CIS					N
S&T	DHS	$100,152	2/22/2005	6/21/2005	Providing admin support to HHS	Y
S&T	DHS	$59,464	11/1/2004	6/30/2005	Providing admin support to HHS	Y
S&T	DHS	$117,809	1/14/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/NAC	$100,152	1/31/2005	(1)	Support DNDO Transition Team for Stand-up	N
NCR	DHS/ODP	$135,136	Unknown	(1)	Nat Cap Reg mission support	N
OSLGC	DHS/ODP	$84,751	2/7/2005	8/6/2005	Support to OSLGCP	N
OSLGC	DHS/ODP	$100,152	2/7/2005	8/6/2005	Support to OSLGCP	N
S&T	DHS/ODP	$117,809	2/7/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$117,809	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,152	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	3/1/2005	(1)	Support DNDO Transition Team for Stand-up	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
FLETC	Federal Air Marshal Service	$96,474	2/7/2005	2/7/2006	On the job Training	N
FLETC	Federal Protective Service	$68,651	10/1/2003	10/1/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	10/20/2003	10/20/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	11/1/2003	11/1/2006	Instructor	N
IAIP	FEMA	$114,882			Support to IAIP mission	N
IAIP	FEMA	$135,136			Support to IAIP mission	N
OSLGC	FEMA	13/3	1/27/2003	TBD	Support to State and Local Coordination and Outreach	N
USM/CFO	FEMA	$100,152	8/1/2004	5/1/2005	Support GAO/IG Liaison Office	N
USM/CHCO	FEMA	$84,751	5/3/2004	1/31/2005	Design of new DHS Personnel HR management system	N
ODP	FEMA/Region III	$82,259	7/11/2004	(1)	Implementation of ODP Program into DHS—move from FEMA Citizen Corp Assistance.	
BTS	FLETC	$100,152	8/1/2003	8/1/2005	FLETC Liaison	N
USM/CFO	FLETC	$100,152	2/1/2005	2/1/2006	Support eMerge project	N
BTS	ICE	$100,152	4/12/2004	4/12/2006	Immigration Policy Advisor	N
BTS	ICE	$117,809	3/10/2003	(1)	Immigration Policy Advisor	N
BTS	ICE	$49,145	11/30/2004	(1)	Protective detail	N
BTS	ICE	$44,495	10/22/2003	(1)	Scheduling Support for Under Secretary	N
BTS	ICE	$69,000	3/14/2005	9/15/2005	FAMS Liaison	N
BTS	ICE	$84,751	9/2/2003	(1)	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	(1)	Advance Work for Under Secretary	Y
BTS	ICE	$49,145	2/27/2005	6/25/2005	Protective detail	N
BTS	ICE	$100,152	8/3/2004	8/3/2005	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	(1)	Advance Work for Under Secretary	Y
BTS	ICE	$100,152	7/1/2004	7/1/2005	Setting up office w/detailees from bureaus (Office of Screening and Coordination).	
CBP	ICE	$100,152	1/1/2005	(1)	Liaison to NTC	N
CBP	ICE	$84,751	12/15/2003	(1)	ICE Liaison	N
CIS	ICE	$59,464	4/1/2004	(1)	Long-term detail to provide paralegal services	N
DHS	ICE	$100,152	7/1/2004	7/1/2005	DHS/CFO	N
DHS	ICE	$117,809	9/1/2003	9/1/2006	Rep to Interpol as Dep Dir for OIA	
FEMA	ICE	$49,145	8/1/2004	(1)	Protective detail	N
FLETC	ICE	$81,638	9/19/2004	9/19/2009	Instructor	N
FLETC	ICE	$81,638	1/15/2003	(1)	Instructor	N
FLETC	ICE	$81,638	5/20/1996	(1)	Instructor	N
FLETC	ICE	$81,638	3/1/1988	(1)	Instructor	N
FLETC	ICE	$81,638	3/1/2001	(1)	Instructor	N
FLETC	ICE	$81,638	9/1/2004	9/1/2007	Instructor	N

FLETC	ICE	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	ICE	$81,638	3/10/2002	3/1/2007	Instructor	N
FLETC	ICE	$81,638	1/23/2003	12/6/2006	Instructor	N
FLETC	ICE	$81,638	11/4/2001	11/4/2006	Instructor	N
FLETC	ICE	$81,638	9/8/2003	9/7/2006	Instructor	N
FTTTF	ICE	$100,152	1/1/2003	(1)	Liaison; NSEERS Tracking	N
IAIP	ICE	$100,152	7/1/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$100,152	1/1/2004	(1)	Interpol Liaison	N
IAIP	ICE	$100,152	1/12/2004	(1)	Serve as ICE rep and subject matter expert	.....
IAIP	ICE	$100,152	11/1/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	(1)	ICE/BTS Liaison	N
IAIP	ICE	$100,152	1/1/2004	(1)	Interpol Liaison	N
IAIP	ICE	$100,152	1/11/2004	(1)	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2004	(1)	Support to IAIP mission	N
IAIP	ICE	$100,152	6/1/2004	6/1/2006	ICE Liaison	Y
IAIP	ICE	$100,152	Jan. 2000	(1)	Support to IAIP mission—DOS Liaison	N
IAIP	ICE	$69,000	7/4/2005	(1)	Intelligence Sharing HSOC	N
IAIP	ICE	$100,152	3/1/2003	3/1/2006	Support to IAIP mission—DHS Liaison to FBI	N
IAIP	ICE	$117,809	2/19/2002	(1)	Support to IAIP mission—HSOC	Y
IAIP	ICE	$100,152	11/1/2003	(1)	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2003	(1)	Support to IAIP mission—HSOC desk officer	N
IAIP	ICE	$100,152	3/1/2003	(1)	Support to IAIP mission	N
ICE	ICE	$84,751	3/1/2002	(1)	ICE Liaison	N
OLA	ICE	$84,751	1/1/2004	(1)	Leg Affairs liaison to Immigration	N
OPA	ICE	$100,152	1/1/2003	(1)	Support to Public Affairs	N
USCG	ICE	$100,152	8/1/2004	(1)	Coast Guard Liaison	N
USM/CIO	ICE	.....	7/12/04	7/8/05	Provide on-site geospatial technical support	N
USM/CIO	ICE	$100,152	12/1/2003	(1)	Program management and acquisition support	N
USM/CIO	ICE	$117,809	10/1/2003	(1)	Director, Infrastructure Transformation Office	N
BTS	TSA	$56,600	6/7/2004	6/7/2005	Provides admin support services to the AA at BTS	N
BTS	TSA	SW–02	2/1/2004	(1)	BTS Deputy Chief of Staff	N
BTS	TSA	$69,000	2/17/2004	(1)	Transportation Security Policy Advisor	N
BTS	TSA	$84,150	12/13/2004	12/13/2005	TSA Liaison	N
BTS	TSA	$84,150	12/31/2004	12/13/2005	Serves as TSA liaison to BTS	N
BTS	TSA	$69,000	7/26/2004	4/2/2005	Provides legislative policy assistance to AA	N
BTS	TSA	$38,900	2/28/2005	10/4/2005	Correspondence Analyst	N
BTS	TSA	$100,600	8/11/2003	8/11/2006	International Affairs	N
BTS	TSA	$100,600	3/23/2003	(1)	National Counter Terrorist Center on SpecialProject	N
BTS	TSA	$46,400	2/2/2004	(1)	Speech Writer	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
BTS	TSA	$84,150	3/7/2005	(1)	Special Asst to Under Secretary	N
BTS	TSA	$100,600	9/26/2004	9/26/2005	Establishing the Office of Screening Coordination for DHS/BTS	N
DHS–OPL	TSA	$84,150	2/13/2005	6/13/2005	Serves as a special assistant for senior level officials TOPOFF3 Program	N
IAIP	TSA	$84,150	3/1/2003	(1)	Support to IAIP mission	N
IAIP	TSA	$69,000	10/1/2003	(1)	Support to IAIP mission	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Task force to review ICE budget	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$84,150	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Assisting with ICE budget audit	N
OGC	TSA	$84,150	8/8/2005	8/8/2007	Provide legal advice concerning border and transportation security issues especially as they involve TSA.	N
OPA	TSA	$84,150	3/3/2003	(1)	Public Affairs assisting on special project (requested by Dennis Murphy)	N
Security	TSA	$100,600	12/12/2004	4/2/2005	Requested for special project on security initiatives at the Chief Security Office.	N
USM	TSA	$120,250	12/26/2004	(1)	Acting Deputy Director Business Transformation office—Selected for DHS position, awaiting clearance through security process.	N
USM	TSA	$158,568	8/30/2004	9/30/2005	Acting Dir, Business Transformation Off	.....
USM/CFO	TSA	$100,152	10/1/2003	10/1/2005	Support eMerge project	N
USM/CIO	TSA	$149,200	4/3/2005	(1)	Support Solutions Engineering COE	Y
USM/CIO	TSA	$152,824	7/13/2003	4/1/2005	Acting Deputy CIO	Y
USM/CIO	TSA	$141,844	7/13/2003	(1)	DHS/BTS Integration	N
USM/CIO	TSA	$110,278	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$145,482	10/27/2004	(1)	TSA representative to the Information Technology Officer	N
USM/CIO	TSA	$138,093	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$141,454	7/13/2003	(1)	INFRASTRUCTURE program support	Y
IAIP	USCG	$136,490	9/19/2003	9/19/2005	HSC Watch Augmentation	N
OGC	USCG	$82,937	3/1/2005	3/1/2007	Assist with international issues and with Team Telecom/CFIUS legal issues	N
Security	USCG	$56,128	12/1/2004	Ongoing	State and Local Investigations	Y
Security	USCG	$82,937	12/1/2004	(3)	State and Local Investigations	Y
Security	USCG	$71,269	12/1/2004	(3)	State and Local Investigations	Y
Security	USCG	$74,560	12/1/2004	(3)	State and Local Investigations	Y
USM/CFO	USCG	$101,613	8/1/2004	8/1/2005	Support Budget Office	N
USM/CFO	USCG	$82,937	1/5/2005	4/1/2005	ICE Tiger Team	N
USM/CIO	USCG	$156,886	.....	(1)	Support DHS' Infrastructure Transformation Office	Y
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Operations Center	N
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Information Analysis Section	N

ICE	USCIS	$87,244	1/3/2005	(1)	To assist ICE in prosecuting Operation Jakarta Asylum Applications—detail lasts until this case goes to trial.	N
ICE	USCIS	$75,460	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraudinvestigation).	N
ICE	USCIS	$41,361	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$64,981	3/14/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
BTS	USSS	$97,206	2/21/2004	8/21/2005	Border & Transp. Security	N
DHS/IAIP	USSS	$91,315	6/1/2004	12/1/2005	Investigations	N
FEMA	USSS	$91,315	10/17/2004	4/17/2005	DEST Program	N
FLETC	USSS	$68,651	8/1/2003	8/10/2008	Instructor	N
FLETC	USSS	$81,638	3/20/2005	3/20/2008	Instructor	N
FLETC	USSS	$68,651	1/1/2003	1/1/2006	Instructor	N
FLETC	USSS	$58,564	6/1/2000	6/1/2005	Instructor	N
FLETC	USSS	$81,638	2/1/2003	2/1/2006	Instructor	N
FLETC	USSS	$63,040	1/12/2004	1/12/2007	Instructor	N
FLETC	USSS	$81,638	2/9/2004	2/9/2009	Instructor	N
FLETC	USSS	$81,638	10/6/2002	12/6/2005	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2005	Instructor	N
IAIP	USSS	$84,751	10/19/2003	5/29/2005	Nat. CounterTerrorism Ctr	N
IAIP	USSS	UND—LT	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$77,274	3/13/2005	6/11/2005	HS Operations Center	N
IAIP	USSS	$100,152	1/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$114,344	5/7/2004	7/10/2005	Protective Research (IAIP)	N
IAIP	USSS	$40,179	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	UND—Off	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	11/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	5/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$97,206	2/8/2004	8/8/2005	Protective Research (IAIP)	N
IAIP	USSS	$103,947	9/1/2004	9/1/2005	Investigations	N
IAIP	USSS	$87,244	2/27/2005	5/28/2005	HS Operations Center	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$110,878	6/1/2003	(3)	Support to IAIP mission—Investigations	Y
IAIP	USSS	$36,157	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2003	(3)	Support to IAIP mission	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
IAIP	USSS	$74,782	3/6/2005	6/4/2005	HS Operations Center	N
IAIP	USSS	$79,766	5/1/2004	5/1/2005	Investigations	N
IAIP	USSS	$100,152	10/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	1/1/2003	(3)	Support to IAIP mission	N
OSLGC	USSS	$88,000	10/3/2004	4/3/2005	Law Enforcement Liaison	N
S&T	USSS	$100,152	2/1/2003	(1)	Providing technical expertise to S&T	N
S&T	USSS	$97,206	1/1/2003	(1)	Providing technical expertise to S&T—Protective Research (INT)	N
Security	USSS	$97,206	7/21/2003	7/21/2005	Counter Intelligence	N
Security	USSS	$88,000	2/1/2003	(1)	Provides physical security to DHS facilities	N
Security	USSS	$94,000	2/23/2003	8/23/2005	Phy. Sec & Access Ctrl	N
USM/CHCO	USSS	$91,315	3/10/2004	4/1/2005	New HR system: pay and performance team	N
USM/CHCO	USSS	$82,259	2/1/2005	5/16/2005	Hiring and transition response team	N
USM/CIO	BTS	$117,809	6/1/2004	6/1/2005	DHS Infrastructure trans support	N
BTS	CBP	$149,200	7/27/2004	7/27/2005	BTS	N
BTS	CBP	$121,274	9/2/2003	9/2/2005	Cargo/Trade Policy	N
BTS	CBP	$117,809	9/7/2004	9/6/2005	Border Patrol Liaison	N
BTS	CBP	$117,809	2/23/2003	(1)	Counternarcotics Projects	N
BTS	CBP	$100,152	7/27/2004	7/27/2005	CIO Assistant	N
BTS	CBP	$94,260	12/6/2004	12/7/2005	Agency Liaison Officer	N
FLETC	CBP	$81,638	10/7/2002	(1)	Instructor	N
FLETC	CBP	$81,638	5/15/1995	(1)	Instructor	N
FLETC	CBP	$81,638	9/2/2003	9/2/2006	Instructor	N
FLETC	CBP	$68,651	5/1/2004	5/1/2007	Instructor	N
FLETC	CBP	$81,638	2/18/1998	(1)	Instructor	N
FLETC	CBP	$68,651	10/1/2002	(1)	Instructor	N
FLETC	CBP	$81,638	2/16/1993	(1)	Instructor	N
FLETC	CBP	$68,651	5/16/2004	5/16/2007	Instructor	N
FLETC	CBP	$81,638	11/19/2001	(1)	Instructor	N
FLETC	CBP	$81,638	8/13/1998	(1)	Instructor	N
FLETC	CBP	$68,651	10/27/2003	10/27/2008	Instructor	N
FLETC	CBP	$68,651	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	11/6/1990	(1)	Instructor	N
FLETC	CBP	$81,638	(2)	(1)	Instructor	N
FLETC	CBP	$81,638	9/25/2000	(1)	Instructor	N
FLETC	CBP	$81,638	3/22/2004	3/22/2007	Instructor	N
FLETC	CBP	$81,638	12/23/2000	(1)	Instructor	N
FLETC	CBP	$81,638	6/1/1998	(1)	Instructor	N

FLETC	CBP	$81,638	9/29/1997	(1)	Instructor	N
FLETC	CBP	$81,638	1/25/1993	(1)	Instructor	N
FLETC	CBP	$68,651	2/24/2004	(1)	Instructor	N
FLETC	CBP	$81,638	7/30/1997	(1)	Instructor	N
FLETC	CBP	$81,638	8/27/2001	8/27/2006	Instructor	N
FLETC	CBP	$57,280	4/15/2002	4/15/2007	Instructor	N
FLETC	CBP	$68,651	7/14/2003	(1)	Instructor	N
IAIP	CBP	$131,671	10/1/2004	(1)	HSOC	N
IAIP	CBP	$91,315	1/10/2005	7/10/2005	Terrorist Screening Ctr	N
IAIP	CBP	$69,173	11/28/2004	5/17/2005	HSOC	N
IAIP	CBP	$73,364	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$75,460	11/29/2004	5/17/2005	HSOC	N
IAIP	CBP	$62,886	11/17/2003	5/31/2005	Support to IAIP Terrorist Screening Center	N
IAIP	CBP	$77,274	9/12/2003	(1)	HSOC	N
IAIP	CBP	$69,173	12/12/2004	6/14/2005	HSOC	N
IAIP	CBP	$77,274	3/20/2005	3/20/2006	COMSEC	N
ICE	CBP	$52,468	3/21/2005	3/21/2006	Visa Security Program	N
ICE	CBP	$124,274	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$43,724	11/1/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$91,315	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$97,213	5/5/2004	5/5/2005	Visa Security Unit	N
ICE	CBP	$91,315	9/20/2004	6/1/2005	Visa Security Unit	N
ICE	CBP	$68,209	11/17/2004	4/29/2005	Visa Security Unit	N
ICE	CBP	$117,809	12/7/2004	TBD	Assist ICE HR Officer	N
OIA	CBP	$62,886	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$57,715	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OIA	CBP	$64,981	1/15/2005	4/30/2005	Border Security Training Team (Jordan)	N
OPA	CBP	$128,205	1/26/2004	(1)	Public Affairs	N
USCG	CBP	$77,274	8/4/2003	(1)	Support to USCG	N
USM/CFO	CBP	$114,344	1/1/2004	(1)	OCFO	N
USM/CFO	CBP	$103,947	10/20/2003	10/19/2005	Support eMerge project	N
USM/CFO	CBP	$106,044	10/1/2003	10/1/2005	Support eMerge project	N
USM/CHCO	CBP	$100,152	4/28/2004	(1)	New HR system: communications team	N
USM/CIO	CBP	$100,152	5/1/2004	5/1/2005	Infrastructure Transformation Office	N
USM/CIO	CBP	$117,344	11/10/2003	6/30/2005	Program manager—HSDN	N
USM/CIO	CBP	$149,200	10/6/2004	7/31/2005	CIO	N
USM/CIO	CBP	$43,365	11/9/2004	9/15/2005	CIO support	N
S&T	CG	$84,751	6/30/2004	6/30/2007	Providing technical expertise to S&T	Y
OGC	CIS	$110,878	9/1/2003	9/1/2006	Provide substantive immigration expertise to DHS OGC, focusing on issues relating to immigration benefits and related USCIS issues.	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
USM/CIO	CIS	$89,736	3/1/2003	(1)	Support DHS' Infrastructure Transformation Office	N
USM/CIO	CIS					N
S&T	DHS	$100,152	2/22/2005	6/21/2005	Providing admin support to HHS	Y
S&T	DHS	$59,464	11/1/2004	6/30/2005	Providing admin support to HHS	Y
S&T	DHS	$117,809	1/14/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/NAC	$100,152	1/31/2005	(1)	Support DNDO Transition Team for Stand-up	N
OSLGC	DHS/ODP	$84,751	2/7/2005	8/6/2005	Support to OSLGCP	N
OSLGC	DHS/ODP	$100,152	2/7/2005	8/6/2005	Support to OSLGCP	N
S&T	DHS/ODP	$117,809	2/7/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$117,809	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,152	1/10/2005	(1)	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	1/10/2005	Indefinite	Support DNDO Transition Team for Stand-up	N
S&T	DHS/TSA	$100,600	3/1/2005	Indefinite	Support DNDO Transition Team for Stand-up	N
FLETC	Federal Air Marshal Service	$96,474	2/7/2005	2/7/2006	On the job Training	N
FLETC	Federal Protective Service	$68,651	10/1/2003	10/1/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	10/20/2003	10/20/2006	Instructor	N
FLETC	Federal Protective Service	$68,651	11/1/2003	11/1/2006	Instructor	N
OSLGC	FEMA	13/3	1/27/2003	TBD	Support to State and Local Coordination and Outreach	N
USM/CFO	FEMA	$100,152	8/1/2004	5/1/2005	Support GAO/IG Liaison Office	N
ODP	FEMA/Region III	$82,259	7/11/2004	Indefinite	Implementation of ODP Program into DHS—move from FEMA Citizen Corp Assistance.	N
BTS	FLETC	$100,152	8/1/2003	8/1/2005	FLETC Liaison	N
USM/CFO	FLETC	$100,152	2/1/2005	2/1/2006	Support eMerge project	N
BTS	ICE	$100,152	4/12/2004	4/12/2006	Immigration Policy Advisor	N
BTS	ICE	$117,809	3/10/2003	Indefinite	Immigration Policy Advisor	N
BTS	ICE	$49,145	11/30/2004	Indefinite	Protective detail	N
BTS	ICE	$44,495	10/22/2003	Indefinite	Scheduling Support for Under Secretary	N
BTS	ICE	$69,000	3/14/2005	9/15/2005	FAMS Liaison	N
BTS	ICE	$84,751	9/2/2003	Indefinite	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	Indefinite	Advance Work for Under Secretary	Y
BTS	ICE	$49,145	2/27/2005	6/25/2005	Protective detail	N
BTS	ICE	$100,152	8/3/2004	8/3/2005	ICE Liaison	N
BTS	ICE	$71,269	6/29/2003	Indefinite	Advance Work for Under Secretary	Y
BTS	ICE	$100,152	7/1/2004	7/1/2005	Setting up office w/ detailees from bureaus (Office of Screening and Coordination).	N
CBP	ICE	$100,152	1/1/2005	Indefinite	Liaison to NTC	N
CBP	ICE	$84,751	12/15/2003	Indefinite	ICE Liaison	N

CIS	ICE	$59,464	4/1/2004	Indefinite	Long-term detail to provide paralegal services	N
DHS	ICE	$100,152	7/1/2004	7/1/2005	DHS/CFO	N
DHS	ICE	$117,809	9/1/2003	9/1/2006	Rep to Interpol as Dep Dir for OIA	N
FEMA	ICE	$49,145	8/1/2004	Indefinite	Protective detail	N
FLETC	ICE	$81,638	9/19/2004	9/19/2009	Instructor	N
FLETC	ICE	$81,638	1/15/2003	Indefinite	Instructor	N
FLETC	ICE	$81,638	5/20/1996	Indefinite	Instructor	N
FLETC	ICE	$81,638	3/1/1988	Indefinite	Instructor	N
FLETC	ICE	$81,638	3/1/2001	Indefinite	Instructor	N
FLETC	ICE	$81,638	9/1/2004	9/1/2007	Instructor	N
FLETC	ICE	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	ICE	$81,638	3/10/2002	3/1/2007	Instructor	N
FLETC	ICE	$81,638	1/23/2003	12/6/2006	Instructor	N
FLETC	ICE	$81,638	11/4/2001	11/4/2006	Instructor	N
FLETC	ICE	$81,638	9/8/2003	9/7/2006	Instructor	N
IAIP	ICE	$100,152	7/1/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$100,152	1/1/2004	Indefinite	Interpol Liaison	N
IAIP	ICE	$100,152	1/12/2004	Indefinite	Serve as ICE rep and subject matter expert	N
IAIP	ICE	$100,152	11/1/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$71,269	8/24/2003	Indefinite	ICE/BTS Liaison	N
IAIP	ICE	$100,152	1/1/2004	Indefinite	Interpol Liaison	N
IAIP	ICE	$100,152	1/11/2004	Indefinite	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2004	Indefinite	Support to IAIP mission	N
IAIP	ICE	$100,152	6/1/2004	6/1/2006	ICE Liaison	Y
IAIP	ICE	$100,152	Jan. 2000	Indefinite	Support to IAIP mission—DOS Liaison	N
IAIP	ICE	$69,000	7/4/2005	Indefinite	Intelligence Sharing HSOC	N
IAIP	ICE	$100,152	3/1/2003	3/1/2006	Support to IAIP mission—DHS Liaison to FBI	N
IAIP	ICE	$117,809	2/19/2002	Indefinite	Support to IAIP mission—HSOC	Y
IAIP	ICE	$100,152	11/1/2003	Indefinite	Support to IAIP mission	N
IAIP	ICE	$84,751	1/1/2003	Indefinite	Support to IAIP mission—HSOC desk officer	N
IAIP	ICE	$100,152	3/1/2003	Indefinite	Support to IAIP mission	N
ICE	ICE	$84,751	3/1/2002	Indefinite	ICE Liaison	N
OLA	ICE	$84,751	1/1/2004	Indefinite	Leg Affairs liaison to Immigration	N
OPA	ICE	$100,152	1/1/2003	Indefinite	Support to Public Affairs	N
USCG	ICE	$100,152	8/1/2004	Indefinite	Coast Guard Liaison	N
USM/CIO	ICE	.....	7/12/04	7/8/05	Provide on-site geospatial technical support	N
USM/CIO	ICE	$100,152	12/1/2003	Indefinite	Program management and acquisition support	N
USM/CIO	ICE	$117,809	10/1/2003	Indefinite	Director, Infrastructure Transformation Office	N
BTS	TSA	$56,600	6/7/2004	6/7/2005	Provides admin support services to the AA at BTS	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
BTS	TSA	SW–02	2/1/2004	Indefinite	BTS Deputy Chief of Staff	N
BTS	TSA	$69,000	2/17/2004	Indefinite	Transportation Security Policy Advisor	N
BTS	TSA	$84,150	12/13/2004	12/13/2005	TSA Liaison	N
BTS	TSA	$84,150	12/31/2004	12/13/2005	Serves as TSA liaison to BTS	N
BTS	TSA	$100,600	7/13/2003	1/22/2005	Operations Executive Assistant	N
BTS	TSA	$69,000	7/26/2004	4/2/2005	Provides legislative policy assistance to AA	N
BTS	TSA	$38,900	2/28/2005	10/4/2005	Correspondence Analyst	N
BTS	TSA	$100,600	8/11/2003	8/11/2006	International Affairs	N
BTS	TSA	$100,600	3/23/2003	Indefinite	National Counter Terrorist Center on special project	N
BTS	TSA	$46,400	2/2/2004	Indefinite	Speech Writer	N
BTS	TSA	$84,150	3/7/2005	Indefinite	Special Asst to Under Secretary	N
BTS	TSA	$100,600	9/26/2004	9/26/2005	Establishing the Office of Screening Coordination for DHS/BTS	N
DHS–OPL	TSA	$84,150	2/13/2005	6/13/2005	Serves as a special assistant for senior level officials TOPOFF3 Program	N
IAIP	TSA	$84,150	3/1/2003	Indefinite	Support to IAIP mission	N
IAIP	TSA	$69,000	10/1/2003	Indefinite	Support to IAIP mission	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Task force to review ICE budget	N
ICE	TSA	$100,600	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$84,150	5/30/2004	5/30/2005	Provide legal support to FAMS at ICE	N
ICE	TSA	$100,600	1/10/2005	4/9/2005	Assisting with ICE budget audit	N
OGC	TSA	$84,150	8/8/2005	8/8/2007	Provide legal advice concerning border and transportation security issues especially as they involve TSA.	N
OPA	TSA	$84,150	3/3/2003	Indefinite	Public Affairs assisting on special project(requested by Dennis Murphy)	N
Security	TSA	$100,600	12/12/2004	4/2/2005	Requested for special project on security initiatives at the Chief Security Office.	N
USM	TSA	$120,250	12/26/2004	Indefinite	Acting Deputy Director Business Transformation office—Selected for DHS position, awaiting clearance through security process.	N
USM	TSA	$158,568	8/30/2004	9/30/2005	Acting Dir, Business Transformation Off	N
USM/CFO	TSA	$100,152	10/1/2003	10/1/2005	Support eMerge project	N
USM/CIO	TSA	$149,200	4/3/2005	Indefinite	Support Solutions Engineering COE	Y
USM/CIO	TSA	$152,824	7/13/2003	4/1/2005	Acting Deputy CIO	Y
USM/CIO	TSA	$141,844	7/13/2003	Indefinite	DHS/BTS Integration	N
USM/CIO	TSA	$110,278	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$145,482	10/27/2004	Indefinite	TSA representative to the Information Technology Officer	N
USM/CIO	TSA	$138,093	4/3/2005	9/30/2005	Information Technology	Y
USM/CIO	TSA	$141,454	7/13/2003	Indefinite	INFRASTRUCTURE program support	Y
IAIP	USCG	$136,490	9/19/2003	9/19/2005	HSC Watch Augmentation	N

OGC	USCG	$82,937	3/1/2005	3/1/2007	Assist with international issues and with Team Telecom/CFIUS legal issues	N
USM/CFO	USCG	$101,613	8/1/2004	8/1/2005	Support Budget Office	N
USM/CFO	USCG	$82,937	1/5/2005	4/1/2005	ICE Tiger Team	N
USM/CIO	USCG	$156,886		Indefinite	Support DHS' Infrastructure Transformation Office	Y
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Operations Center	N
IAIP	USCIS	$74,782	3/21/2005	5/21/2005	To assist in setting up DHS' Information Analysis Section	N
ICE	USCIS	$87,244	1/3/2005	Indefinite	To assist ICE in prosecuting Operation Jakarta Asylum Applications—detail lasts until this case goes to trial.	N
ICE	USCIS	$75,460	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$81,747	2/28/2005	3/4/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$41,361	3/7/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
ICE	USCIS	$64,981	3/14/2005	5/6/2005	To assist ICE in prosecuting Operation Jakarta Asylum Applications (a 2 year asylum fraud investigation).	N
BTS	USSS	$97,206	2/21/2004	8/21/2005	Border & Transp. Security	N
DHS/IAIP	USSS	$91,315	6/1/2004	12/1/2005	Investigations	N
FEMA	USSS	$91,315	10/17/2004	4/17/2005	DEST Program	N
FLETC	USSS	$68,651	8/1/2003	8/10/2008	Instructor	N
FLETC	USSS	$81,638	3/20/2005	3/20/2008	Instructor	N
FLETC	USSS	$68,651	1/1/2003	1/1/2006	Instructor	N
FLETC	USSS	$58,564	6/1/2000	6/1/2005	Instructor	N
FLETC	USSS	$81,638	2/1/2003	2/1/2006	Instructor	N
FLETC	USSS	$63,040	1/12/2004	1/12/2007	Instructor	N
FLETC	USSS	$81,638	2/9/2004	2/9/2009	Instructor	N
FLETC	USSS	$81,638	10/6/2002	12/6/2005	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2006	Instructor	N
FLETC	USSS	$81,638	9/1/2003	9/1/2005	Instructor	N
IAIP	USSS	$84,751	10/19/2003	5/29/2005	Nat. CounterTerrorism Ctr	N
IAIP	USSS	UND—LT	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$77,274	3/13/2005	6/11/2005	HS Operations Center	N
IAIP	USSS	$100,152	1/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$114,344	5/7/2004	7/10/2005	Protective Research (IAIP)	N
IAIP	USSS	$40,179	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	UND—Off	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	11/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	5/1/2003	(3)	Support to IAIP mission	N

Detailed To	Originating Agency	Grade/Step or Salary	Detail Start Date	Detail End Date	Purpose of Detail	Reimbursable Y/N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$97,206	2/8/2004	8/8/2005	Protective Research (IAIP)	N
IAIP	USSS	$103,947	9/1/2004	9/1/2005	Investigations	N
IAIP	USSS	$87,244	2/27/2005	5/28/2005	HS Operations Center	N
IAIP	USSS	$84,751	12/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$110,878	6/1/2003	(3)	Support to IAIP mission—Investigations	Y
IAIP	USSS	$36,157	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	12/1/2003	(3)	Support to IAIP mission	N
IAIP	USSS	$74,782	3/6/2005	6/4/2005	HS Operations Center	N
IAIP	USSS	$79,766	5/1/2004	5/1/2005	Investigations	N
IAIP	USSS	$100,152	10/1/2002	(3)	Support to IAIP mission	N
IAIP	USSS	$84,751	1/1/2004	(3)	Support to IAIP mission	N
IAIP	USSS	$117,809	1/1/2003	(3)	Support to IAIP mission	N
OSLGC	USSS	$88,000	10/3/2004	4/3/2005	Law Enforcement Liaison	N
S&T	USSS	$100,152	2/1/2003	Indefinite	Providing technical expertise to S&T	N
S&T	USSS	$97,206	1/1/2003	Indefinite	Providing technical expertise to S&T—Protective Research (INT)	N
Security	USSS	$97,206	7/21/2003	7/21/2005	Counter Intelligence	N
Security	USSS	$88,000	2/1/2003	Indefinite	Provides physical security to DHS facilities	N
Security	USSS	$94,000	2/23/2003	8/23/2005	Phy. Sec & Access Ctrl	N
USM/CHCO	USSS	$91,315	3/10/2004	4/1/2005	New HR system: pay and performance team	N
USM/CHCO	USSS	$82,259	2/1/2005	5/16/2005	Hiring and transition response team	N

[1] Indefinite.
[2] N/A.
[3] Ongoing.

HIRING JOURNALISTS

Question. In January 2005, President Bush ordered his Cabinet secretaries not to hire columnists to promote their agendas. At a news conference President Bush said, "All our Cabinet secretaries must realize that we will not be paying commentators to advance our agenda. Our agenda ought to be able to stand on its own two feet."

Are all DHS agencies in compliance with the Administration's policy and the legal prohibitions on using appropriations for contracting with journalists to promote legislation or policy?

Answer. Yes, all DHS Agencies are in compliance.

INTELLIGENCE REFORM BILL AUTHORIZATIONS

Question. The Intelligence Reform and Terrorism Prevention Act authorized substantial enhancements to a variety of DHS programs, including immigration enforcement, aviation security, and other provisions. Identify the funding requested in the President's fiscal year 2006 budget for each of the following authorizations contained in the Act. In your response, include a chart which compares the funding authorized, by section of the bill, to the funding included in the President's fiscal year 2006 budget.

Immigration Enforcement

—*Section 5202 & 5203.*—Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 10,000 additional Border Patrol Agents (2,000 per year) and an increase of 4,000 Immigration and Customs Enforcement (ICE) investigators (800 per year).

—*Section 5204.*—Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 40,000 beds (8,000 per year) available for immigration detention and removal.

—*Section 5101 through 5104.*—The Secretary of Homeland Security may carry out a pilot program to improve border security between ports of entry along the northern border. Required features of this pilot project include the use of advanced technologies to improve border security.

—*Section 5201.*—Within 6 months of enactment of this Act, the Secretary of Homeland Security shall submit a comprehensive plan for the systematic surveillance of the southwest border of the United States by remotely piloted aircraft.

—*Section 7210 & 7206.*—The bill amends the Immigration and Nationality Act by mandating by January 1, 2008 pre-inspection stations are established in at least 25 additional foreign airports and by December 31, 2006 at least 50 airports shall be selected for assignment of immigration officers to assist air carriers detect fraudulent documents at foreign airports. $25 million is authorized in fiscal year 2005 and $40 million in fiscal years 2006 and 2007 respectively for this purpose.

Aviation Security

—*Section 4013.*—$250 million for research, development, and installation of detection systems and other devices for the detection of biological, chemical, radiological, and explosive material.

—*Section 4024.*—$100 million for research and development of improved explosive detection systems.

—*Section 4052.*—$200 million for each of fiscal years 2005–2007 for improving aviation security related to the transportation of cargo on passenger and cargo aircraft.

—*Section 4052.*—$100 million for each of fiscal years 2005–2007 for research and development in advancing cargo security technology. Within these funds, the Secretary shall also establish a competitive grant program to encourage the development of advanced air cargo security technology.

—*Section 4014.*—Up to $150 million for each of fiscal years 2005 and 2006 to set up a pilot program (minimum 5 airports) to deploy and test advanced airport checkpoint screening devices and technology as an integrated system.

—*Section 4019.*—Increases the statutory allocation for expiring and new Letters of Intent (LOIs) from $250 million to $400 million.

—*Section 4011.*—$20 million for research and development of advanced biometric technology applications to aviation security, including mass identification technology.

—*Section 4011.*—$1 million for the establishment of a competitive center of excellence to expedite the use of biometric identifiers.

—*Section 4011.*—Directs that a law enforcement officer travel credential be created that incorporates biometric identifier technology that is uniform for all law enforcement officials seeking to carry a weapon on board an aircraft. The bill authorizes such sums as may be necessary to carry out this directive.

—*Section 4020.*—Directs DHS to provide, subject to the availability of funds, monitoring cameras for surveillance at airports that have checked baggage screening areas that are not open to public view in order to deter theft from checked baggage and to aid in the speedy resolution of liability claims against the Transportation Security Administration.

—*Section 4051.*—$2 million for TSA to carry out a pilot program to evaluate the use of blast-resistant containers for cargo and baggage on passenger aircraft to minimize the potential effects of detonation of an explosive device.

—*Section 4016.*—$83 million for the 3 fiscal-year period beginning with fiscal year 2005 to increase the number of Federal air marshals.

—*Section 4012.*—Directs TSA to begin to assume the function (not later than 180 days after testing the system is completed) of comparing passenger information to no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist, including international flights.

Other Provisions

—*Section 7303.*—Authorizes the Secretary of DHS to provide $22.1 million in fiscal year 2005, $22.8 million in fiscal year 2006, $23.5 million in fiscal year 2007, $24.2 million in fiscal year 2008, and $24.9 million in fiscal year 2009 to enhance public safety interoperable communications at all levels of government. The Secretary may establish an Office for Interoperability and Compatibility within the Science and Technology Directorate to carry out these duties.

—*Section 7304.*—Directs DHS to establish a minimum of 2 pilot projects in high threat urban areas or regions for the purpose of developing a regional strategic plan to foster interagency communication and to coordinate the gathering of all Federal, State, and local first responders in that area.

—*Section 7407.*—Amends the Homeland Security Act requirement related to counternarcotics enforcement. Instead of having one senior official in the Department coordinating counternarcotics policy, an "Office Counternarcotics Enforcement" is created with an authorization of $6 million.

—*Section 7215.*—Directs the Secretary to establish a terrorist travel program to oversee the analysis, coordination, and dissemination or terrorist travel intelligence and operation information.

—*Section 4071.*—Directs the Secretary to implement a system for screening the names of cruise ship passengers and crew against Federal terrorist watch lists.

Answer.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY

Subject area	Authorized Funding Level	2006 Budget Funding Level
AVIATION:		
Law enforcement officer uniform biometric travel credential (Section 4011(a)).	Directs that a law enforcement officer travel credential be created that incorporates biometric identifier technology that is uniform for all law enforcement officials seeking to carry a weapon on board an aircraft. The bill authorizes such sums as may be necessary to carry out this directive.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose. Necessary resources would be provided with existing funds or through fees. This activity is a sub-set of the Registered Traveler pilot and funds were identified within the Registered Traveler program in fiscal year 2005 to begin the Registered Armed LEO pilot. The fiscal year 2005 enacted appropriations funded Registered Armed LEO activities, and TSA anticipates using the results of the pilot as a platform for the final LEO biometric travel card. Results of the pilot will be considered to evaluate resources, needs, and funding options as the program moves forward.
Biometric technologies for aviation—R&D (Section 4011(b))	$20 million for research and development of advanced biometric technology applications to aviation security, including mass identification technology.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose within broader R&D request levels.
Biometric Center of Excellence (Section 4011(d))	$1 million for the establishment of a competitive center of excellence to expedite the use of biometric identifiers.	The fiscal year 2006 Budget does not request any dedicated funding for a Biometric Center of Excellence.
Airline Passenger Screening (Section 4012)	Directs TSA to begin to assume the function (not later than 180 days after testing the system is completed) of comparing passenger information to no fly lists, utilizing all appropriate records in the consolidated and integrated terrorist watchlist, including international flights.	The fiscal year 2006 Budget requests $81 million for the development of the Secure Flight prescreening system.
Checkpoint portal detection systems—R&D and deployment (Section 4013).	$250 million for research, development, and installation of detection systems and other devices for the detection of biological, chemical, radiological, and explosive material.	The fiscal year 2006 Budget for explosives detection as a countermeasure against aviation, suicide and vehicle bombs: $88 million of the $124 million (Research and Development (R&D) consolidation budget + Science and Technology (S&T) Explosives Countermeasures portfolio budget), but nothing specific for ''checkpoint portal detection systems''.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY—Continued

Subject area	Authorized Funding Level	2006 Budget Funding Level
Integrated checkpoint screening system pilots (Section 4014)	Up to $150 million for each of fiscal years 2005 and 2006 to set up a pilot program (minimum 5 airports) to deploy and test advanced airport checkpoint screening devices and technology as an integrated system.	The President's fiscal year 2005 Budget included $28.3 million for fielding emerging technology equipment at checkpoints. As a result of this funding, 147 static trace portals (which are passenger screening sub-systems using a whole body portal to inspect passengers for concealed explosives using an automated, non-contact trace sampling and processing system) will be deployed in fiscal year 2006 at approximately 40 airports. The fiscal year 2006 request includes $43.7 million in additional funds to complete the fielding of this capability, which will total $100 million to address this activity over the 2-year period.
In-line checked baggage screening (Section 4019)	Increases the statutory allocation for expiring and new Letters of Intent (LOIs) from $250 million to $400 million.	The fiscal year 2006 Budget includes $260.5 million to support the eight existing Letters of Intent (LOI) airports. Of this amount, $240.5 million is for direct reimbursements and $20 million is for equipment and installation. The fiscal year 2006 request proposes to continue sourcing LOIs from the $250 million appropriated from the Aviation Security Capital Fund at a 75 percent Federal cost share rate. Additionally, the request includes $134 million to purchase and install Explosive Detection Systems and Electronic Trace Detection equipment at non-LOI airports, for a total expenditure of $394 million.
Checked Baggage Monitoring Area (Section 4020)	Directs DHS to provide, subject to the availability of funds, monitoring cameras for surveillance at airports that have checked baggage screening areas that are not open to public view in order to deter theft from checked baggage and to aid in the speedy resolution of liability claims against the Transportation Security Administration. The bill and current policy provides "such sums".	The fiscal year 2006 Budget includes $10.1 million to provide assistance to airports to install security monitoring cameras for surveillance of checked baggage screening areas that are not open to public view. The Transportation Security Administration (TSA), in partnership with airports, generally provides for purchase and installation of a camera system, with the partnering airport agreeing to maintain the installed system.
Aviation explosives detection equipment R&D (Section 4024(b))	$100 million for research and development of improved explosive detection systems.	The S&T Directorate has an fiscal year 2006 budget request of $45.9 million for the TSA budget line for next generation explosives detection systems. The S&T Directorate will coordinate with TSA regarding the development of the next generation of explosives detection systems.

Blast Resistant Cargo Containers (Section 4051)	$2 million for TSA to carry out a pilot program to evaluate the use of blast-resistant containers for cargo and baggage on passenger aircraft to minimize the potential effects of detonation of an explosive device.	The fiscal year 2006 Budget requests $4.4 million.
Air cargo security activities (Section 4052)	$200 million for each of fiscal years 2005–2007 for improving aviation security related to the transportation of cargo on passenger and cargo aircraft. $100 million for each of fiscal years 2005–2007 for research and development in advancing cargo security technology. Within these funds, the Secretary shall also establish a competitive grant program to encourage the development of advanced air cargo security technology.	The fiscal year 2006 Budget includes $40 million for air cargo security, which will allow the Transportation Security Administration (TSA) to continue making incremental and measured progress toward our air cargo security goals. The S&T Directorate has an fiscal year 2006 budget request of $29.578 million. The budget request, although not developed by the S&T Directorate, was agreed upon by the S&T Directorate as the amount moving forward for air cargo RDT&E. The S&T Directorate will continue to award grants under a competitive process to further aviation consolidated cargo screening RDT&E.
Federal Air Marshals (FAMS) staffing (Section 4016)	$83 million for the 3 fiscal-year period beginning with fiscal year 2005 to increase the number of Federal air marshals. Subject to the availability of appropriations.	The President has requested $9.86 million in new funding in fiscal year 2006 to enable the hiring of additional Federal Air Marshals to provide even greater coverage of targeted critical flights and to otherwise increase mission capabilities. The total budget for FAMS is $689 million.
Pre-clearance Stations and Immigration Security Initiative (Section 7210 & 7206).	The bill amends the Immigration and Nationality Act by mandating by January 1, 2008 pre-inspection stations are established in at least 25 additional foreign airports and by December 31, 2006 at least 50 airports shall be selected for assignment of immigration officers to assist air carriers detect fraudulent documents at foreign airports. $25 million is authorized in fiscal year 2005 and $40 million in fiscal years 2006 and 2007 respectively for this purpose.	There are currently 14 pre-clearance stations funded in the fiscal year 2006 Budget. The fiscal year 2006 Budget request is $2 million

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY—Continued

Subject area	Authorized Funding Level	2006 Budget Funding Level
MARITIME:		
Vetting of cruise ship passengers (Section 4071)	Directs the Secretary to implement a system for screening the names of cruise ship passengers and crew against Federal terrorist watch lists. No specific funding authorization is provided.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose. Necessary resources are provided with existing funds. On April 7, 2005, CBP published the Advance Passenger Information System (APIS) Final Rule within the Federal Register (70 FR 17820). The CBP Final Rule incorporates passenger and crew manifest requirements from CBP with the Notice of Arrival requirements of the United States Coast Guard (USCG). The CBP Final Rule requires that sea carriers electronically submit certain data on all passengers and crew members prior to entry to or departure from the United States. The data that must be provided includes biographical data and vessel information for each passenger or crewmember. Working with the USCG, CBP developed the Electronic Notice of Arrival/Departure System (eNOA/D), an Internet portal available on the National Vessel Movement Center (NVMC) web site. Using this portal, commercial vessel owners, operators or agents can transmit one electronic message and comply with the CBP APIS requirement for passengers and crew and the USCG Notice of Arrival requirements for vessels. eNOA/D became operational and available to the industry during February 2005. CBP's efforts on the eNOA/D system have been accomplished with existing funds.

BORDER PROTECTION:		
Advanced Technology Northern Border Security Program (Section 5101–5104).	The Secretary of Homeland Security may carry out a pilot program to improve border security between ports of entry along the northern border. Required features of this pilot project include the use of advanced technologies to improve border security. There is authorized to be appropriated "such sums as may be necessary to carry out the pilot program".	The fiscal year 2006 Budget does not request any dedicated funding for a specific pilot. Necessary resources will be provided with existing funds. The fiscal year 2006 Budget requested funding for $19.8 million added to the base funding of $31.3 million to improve border security using advanced technologies on both the northern and southern land borders. Also included in the fiscal year 2006 CBP budget are $20 million for aircraft recapitalization, $10 million in base funding for UAVs, and funding for technical infrastructure. The America's Shield Initiative (ASI) program will evaluate and determine the optimal mix of technology for meeting security requirements of both land borders.
Border surveillance (Section 5201)	Within 6 months of enactment of this Act, the Secretary of Homeland Security shall submit a comprehensive plan for the systematic surveillance of the southwest border of the United States by remotely piloted aircraft. The Secretary of Homeland Security shall implement the plan as a pilot program as soon as sufficient funds are appropriated and available for this purpose.	The fiscal year 2006 Budget requests $10 million for unmanned aerial vehicles.
Border Patrol agents (Section 5202)	Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 10,000 additional Border Patrol Agents (2,000 per year).	The fiscal year 2006 Budget requests 210 new agents and $36.9 million.
ENFORCEMENT:		
Immigration and Customs Enforcement investigators (Section 5203)	Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 4,000 Immigration and Customs Enforcement (ICE) investigators (800 per year). Subject to the availability of appropriations.	The fiscal year 2006 Budget requests 150 agents and $18 million.
Detention bed space (Section 5204)	Authorizes, from fiscal year 2006 to fiscal year 2010 subject to the availability of appropriations, an increase of 40,000 beds (8,000 per year) available for immigration detention and removal. Subject to the availability of appropriations.	The fiscal year 2006 Budget includes an increase of $90 million for detention beds and detention and removal officers. This increase will fund 1,920 beds. Overall, the fiscal year 2006 Budget provides $1.5 billion for detention and removal activities. The budget also includes an enhancement of $39 million for the detention and repatriation costs of the Arizona Border Control Initiative.

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 IMPLICATIONS FOR THE DEPARTMENT OF HOMELAND SECURITY—Continued

Subject area	Authorized Funding Level	2006 Budget Funding Level
OTHER:		
Public Safety Interoperable Communications (Section 7303)	Authorizes the Secretary of DHS to provide $22.1 million in fiscal year 2005, $22.8 million in fiscal year 2006, $23.5 million in fiscal year 2007, $24.2 million in fiscal year 2008, and $24.9 million in fiscal year 2009 to enhance public safety interoperable communications at all levels of government. The Secretary may establish an Office for Interoperability and Compatibility within the Science and Technology Directorate to carry out these duties.	The fiscal year 2006 Budget requests $20.5 million for the S&T Directorate's Office of Interoperability and Compatibility (OIC) to enhance public safety interoperable communications.
Regional Strategic Plan (Section 7304)	Directs DHS to establish a minimum of 2 pilot projects in high threat urban areas or regions for the purpose of developing a regional strategic plan to foster interagency communication and to coordinate the gathering of all Federal, State, and local first responders in that area.	The fiscal year 2006 Budget requests $20.5 million for the Department of Homeland Security's S&T Directorate's OIC to enhance public safety interoperable communications through SAFECOM, a program of OIC.
Counternarcotics Enforcement (Section 7407)	Amends the Homeland Security Act requirement related to counternarcotics enforcement. Instead of having one senior official in the Department coordinating counternarcotics policy, an ''Office Counternarcotics Enforcement'' is created with an authorization of $6 million.	The fiscal year 2006 request for the Office of Counternarcotics Enforcement is $1.86 million.
Terrorist Travel Program (Section 7215)	Directs the Secretary to establish a terrorist travel program to oversee the analysis, coordination, and dissemination or terrorist travel intelligence and operation information.	The fiscal year 2006 Budget does not request any dedicated funding for this specific purpose. Necessary resources would be provided with existing funds.

MERIT SYSTEM PROTECTION BOARD (MSPB)

Question. The final regulation restricts the ability of the MSPB to mitigate penalties selected by DHS. The final rule says, "Our intent is to explicitly restrict the authority of MSPB to modify those penalties to situations where there is simply no justification for the penalty. MSPB may not modify the penalty imposed by the Department unless such penalty is so disproportionate to the basis for action as to be wholly without justification." This standard is exceptionally high. Why was such a departure from the current authorities of the MSPB necessary?

Answer. Under current MSPB case law, penalties can be mitigated down if they are "unreasonable." Problems with this include that it is subjective and it may result in many employees returning to the workplace after the MSPB "suspension" instead of being removed as recommended by management.

DHS believes that management decisions should be given great deference with regard to discipline, especially with removals, because an undesirable employee returning to the workforce creates morale problems at the least; at the worst, a returning employee interferes with the agency's mission to protect the homeland.

MSPB's ability to mitigate a penalty only if the punishment is "so disproportionate as to be wholly without justification" is a compromise because it gives greater deference to DHS, still protects employee due process, and ensures that disciplinary actions are not initiated irresponsibly.

Question. Is the Department concerned that these extreme measures will adversely affect employee morale and reduce employee confidence that they will be treated fairly?

Answer. DHS understands that many employees are wary of the unknown and is currently in the process of rolling out significant training efforts aimed at communicating with employees, training managers, and executives on the new human resource system and the expectations for those managers regarding the system. Fair treatment is critical to the success of the new system and is a key component of our implementation and ongoing evaluation processes.

Question. What evidence is there that the existing MSPB authorities have adversely affected agency missions?

Answer. The Department's priority homeland security mission requires that it maintain an exceptionally high degree of order and discipline in the workplace. This order and discipline is undermined when disciplinary decisions are mitigated by MSPB judges on the existing "reasonableness" standard. Indeed, the mere threat of such a low standard for mitigation causes agency managers to second guess themselves and hesitate to discipline employees even when such discipline is clearly warranted. The Department has therefore instituted a higher standard for mitigation of penalties aimed at providing managers with the confidence to institute disciplinary actions where required in support of the agency's homeland security mission. To allow very poor performers to continue in the workplace is unacceptable and can negatively affect all agency operations.

CONCERNS OF EMPLOYEES

Question. A number of DHS employees have strong concerns about the final DHS personnel regulations, which were published in the Federal Register on February 1, because the regulations diminish employees due process rights and restrict collective bargaining. What is the Department's opinion on the objections raised by the front line DHS employees, and what will the Department do to address the concerns expressed by these Federal employees?

Answer. The new HR system does maintain due process and is consistent with the Homeland Security Act's promise to preserve collective bargaining rights. It also is responsive to DHS' unique mission needs. DHS understands that employees have concerns about the new human resources systems and has embarked on robust efforts to inform employees and train managers about the new system, including through continuing collaboration with DHS labor unions. Through focus groups, the "Ask MAX" question response system and employee surveys, DHS is keeping a close watch on employee opinions and through the formal program evaluation process will be measuring the results and outcomes of the new system. If necessary, the system can be fine-tuned to make mid-course corrections.

INDEPENDENT REVIEW OF COLLECTIVE BARGAINING DISPUTES

Question. As part of the new personnel regulations, the responsibility for deciding collective bargaining disputes will lie with a three-member internal DHS Labor Relations Board appointed by the Secretary. Currently, throughout the Federal Government, collective bargaining disputes are decided by the Federal Labor Relations

Authority (FLRA), an independent body appointed by the President and confirmed by the Senate. How does DHS/OPM believe that the internal labor relations board meets the statutory mandate of the Homeland Security Act that DHS employees may, "organize, bargain collectively, and participate through labor organizations of their own choosing in decisions which affect them"?

Answer. The Homeland Security Labor Relations Board (HSLRB) is an independent Board similar to the FLRA, but appointed by the Secretary with nominees recommended by the DHS labor organizations. All nominees must be independent citizens who are known for their integrity and impartiality in addition to having expertise in labor relations, law enforcement, or national/homeland or other related security matters. The HSLRB hears cases involving the duty to bargain and the DHS homeland security mission, with the FLRA hearing all other cases (for example, appropriate unit determinations and unfair labor practice charges involving exercise of employee rights) and reviewing the HSLRB's substantive decisions. The FLRA review is then subject to judicial review. These substantive and procedural attributes of the HSLRB ensure that DHS, DHS employees and DHS labor organizations obtain an impartial adjudication of labor relations cases while recognizing the Department's priority homeland security mission.

MANDATORY TERMINATION WITH NO OUTSIDE REVIEW

Question. The final regulations provide the Secretary with discretion to create a list of Mandatory Removal Offenses (MRO) that will only be appealable on the merits to an internal DHS Mandatory Removal Panel (MRP) appointed by the Secretary. In addition, the regulations provide the Secretary with the sole discretion to mitigate a removal penalty. How can the agency expect front line employees to have any confidence in a personnel system where the most serious matters are charged and adjudicated by the Secretary and his appointed "Removal Panel"?

Answer. Currently DHS is taking no action to implement MROs. On August 15, 2005, Judge Collyer of the District Court for the District of Columbia requested that DHS and OPM delay implementation. On August 12, 2005, Judge Collyer issued an order enjoining one provision within the appeals subpart of the regulations but permitting DHS to move forward with the rest of the adverse actions and appeals provisions. The Department and OPM are currently working to set a revised timeline for making the adverse actions and appeals subparts operative in light of the ruling.

TASKING THE FLRA AND MSPB

Question. What particular statutory authority enabled the final regulations to give the FLRA and the MSPB new duties and rules of operation? The FLRA and the MSPB are independent agencies.

Answer. The Homeland Security Act provided an amendment to Title 5, United States Code, that authorized the Secretary of DHS and the Director of OPM to establish a human resources management system for DHS that waives or modifies certain provisions of Title 5. Included among the provisions that can be waived or modified are chapters 71 and 77, which prescribe the operations of the FLRA and MSPB respectively. After consulting with FLRA and MSPB, the Secretary and the Director relied upon this grant of authority, found in 5 U.S.C. 9701, to promulgate regulations that modify chapters 71 and 77 and alter the way the FLRA and MSPB handle DHS cases.

TRAINING OF SUPERVISORS

Question. One of the continuing concerns surrounding the final DHS personnel regulations is the fact that many personnel decisions, especially pay, will now be based on factors under the control of local supervisors and directors. How does DHS plan to address the concerns of front line officers that supervisors, who will be granted a tremendous amount of pay and performance evaluation discretion under the new personnel regulations, will be properly trained to ensure transparency and fairness for all front-line personnel?

Answer. Performance ratings will continue to be determined by local supervisors, just as it occurs in today's performance management process. The concept of a second level reviewing official has been retained as an inherent check and balance. A comprehensive training program will be undertaken to train supervisors and managers to make meaningful distinctions in performance and, just as important, to articulate clear performance expectations, which will be used to track performance. An automated performance management system will make the administration of the system more transparent to employees and will facilitate self-assessment and peer review capabilities that can serve as important information sources for the supervisor's consideration. Additionally, we envision that performance pay pools will be

centrally established and managed at higher organizational levels, thus mitigating the influence of a single supervisor on the pay side of the process. A Department-level Compensation Committee, including DHS union representation, also will have considerable influence on the pay for performance program and its administration.

Question. In addition, this system will take more training and administrative time. How will those increased administrative costs be paid for?

Answer. The vast majority of administrative costs associated with training will be funded through requested appropriations specified for implementation of the new HR system and managed by the DHS Chief Human Capital Office for the Department-wide training initiative. As part of the new system, DHS will provide automated tools, e.g., a new electronic performance management system, to assist management officials in program administration.

Question. Won't resources be taken from frontline Homeland Security positions?

Answer. The expectation is that resources will be provided in requests for appropriations specifically identified to support implementation of the new HR system. Individual Department components' mission budgets are not expected to be impacted. We believe time spent in training on effective performance management and in coaching and providing feedback to employees is time well spent that generates positive returns in overall agency effectiveness.

PAY FOR PERFORMANCE

Question. As you know, DHS employees' pay will be shifting from the current GS-scale pay system to a pay-for-performance system under the new DHS personnel regulations. How can a credible pay-for-performance pay system work in an agency, such as DHS, that requires a tremendous amount of teamwork to successfully accomplish agency missions?

Answer. Performance work plans will contain measurable performance elements that specifically address teamwork or similar concepts for those occupations requiring such attributes. Employees in those occupations will know that performance that demonstrates teamwork will be rewarded.

Question. Is the Department aware of any large scale pay-for-performance system that has been successfully implemented in a law-enforcement environment?

Answer. While we are unaware of a large scale pay-for-performance system in a law enforcement environment, that certainly does not prevent us from developing one. Pay-for-Performance is the concept of providing a pay increase based on "performance" (e.g. achievement of a performance goal or positive performance appraisal rating). Organizations tie pay to performance in various ways. They may base pay on measures of individual, team, or organizational performance. We feel this concept can work well in a law enforcement environment. Research involved in designing the system entails review and evaluation of private, other Federal, State and local systems that have such programs. Our design work includes program evaluation aspects in order to periodically monitor, evaluate, and revise the system, as warranted to ensure that objectives are being attained.

SECURITY AND PROSPERITY PARTNERSHIP OF NORTH AMERICA

Question. On March 23, President Bush held a press event in Waco, Texas with Mexican Pres Foxx and Canadian Prime Minister Martin where he announced a grant program for the Security and Prosperity Partnership of North America.

The parties to the partnership were tasked to set specific, measurable, and achievable goals and implementation dates to develop a common security strategy to further secure North America, including preventing and responding to threats within North America and streamlining the secure and efficient movement of legitimate and low-risk traffic across our shared borders.

Will we be receiving a budget amendment to provide the resources for Customs and Border Patrol, the Coast Guard, and Immigration and Customs Enforcement to implement this partnership or was this announcement an exercise in public relations?

Answer. On March 23, 2005, in Waco, Texas, President Bush, along with Canadian Prime Minister Martin and Mexican President Fox, unveiled the Security and Prosperity Partnership for North America (SPP), a blueprint for a safer and more prosperous continent. The three leaders instructed each nation to establish ministerial-level SPP working groups. I chair the security component, and the prosperity component is chaired by Department of Commerce Secretary Gutierrez. Department of State Secretary Rice is working to ensure the two components are integrated and that the SPP advances U.S. foreign policy goals and enhances our strong relationships with Canada and Mexico.

The SPP will complement, rather than replace, existing bilateral and trilateral fora and working groups that are performing well. The issues of immigration and trade disputes will be dealt with outside the SPP through existing treaties and congressional action.

Following the March 23 announcement, DHS and Commerce conducted a series of Congressional briefings and other stakeholder outreach sessions.

On June 27, I and Gutierrez and our government counterparts in Mexico and Canada released the first report of the SPP that identifies initial results, key themes and initiatives, and work plans that further promote the security and prosperity of the continent.

At this time, DHS anticipates accomplishing the fiscal year 2006 initiatives contained in the SPP within available resources. We would like to reserve the opportunity to address some longer term priorities as part of the normal budgeting process in the future. We continue to be interested in input from the Congress, industry and other stakeholders as we implement the SPP.

DHS REPORTS DUE

Question. In the fiscal year 2005 Homeland Security Appropriations Act and associated reports, Congress directed the Department to report to the Committee on a number of important issues. To date, 70 percent of the reports currently due to the House & Senate Committees on Appropriations have not yet been received. What is the Department's plan for increasing the rate of timely submission of Congressionally required reports?

Answer. The Department continues to place a significant priority on providing timely information and reports to Congress. Of the reports mentioned above, approximately 40 percent of those outstanding reports are past due, and the Department has been working diligently to expedite transmittal of those reports. Since the hearing on April 20th through July 13th, the Department has reduced the overall number of outstanding reports by approximately 30 percent. As of July 13, the Department has submitted 143 reports for fiscal year 2005 to the Congressional Appropriation Committees.

The status of reports is constantly monitored and regular progress is tracked and evaluated. Furthermore, Congressional reports are discussed regularly at several high-level management meetings, including the DHS Management Council, Chief Financial Officers Council, and Budget Officer meetings. In addition, the Department has reviewed and implemented strategies to streamline and improve the clearance process.

CHIEF INFORMATION OFFICER

Question. From the fiscal year 2004 enacted budget to the fiscal year 2006 President's request, the CIO's budget has increased substantially. The President's budget for fiscal year 2006 requests $303.7M for this office. What safeguards has the Department put in place to ensure that this funding has the proper government management and oversight?

Answer. The Department is using two parallel processes to ensure proper governance and management of its funding, the Planning, Programming, Budgeting, and Execution (PPBE) process, mandated by Management Directive (MD) 1330, and the Investment Review Process (IRP), mandated by MD 1400.

The PPBE process has four steps:

—*Planning.*—The Office of the CIO (OCIO) develops information technology (IT) strategic plans and these plans are reviewed to ensure alignment with the Department's overall strategic plan.

—*Programming.*—The OCIO enters its budget year plus 4 years funding requirements into the Future Years Homeland Security Program (FYHSP) system for review, program evaluation, and analysis by Departmental management.

—*Budgeting.*—The OCIO budget is reviewed and the OCIO enters budget justification information for all of its IT investments into the Investment Management System (IMS) for scoring and portfolio review by Departmental management.

—*Execution.*—All spending plans are reviewed before and during the execution year by Departmental management. Also, each individual expenditure is reviewed at multiple Levels within the OCIO and by Departmental management before execution, and is tracked through the Federal Financial Management System (FFMS) and the Procurement Request Information Management System (PRISM).

The Investment Review Process (IRP) consists of a layered review process, depending on the Level and life cycle phase of the investment. Specifically, the IRP consists of the following:

—*Investment Review Board (IRB).*—The IRB provides decision authority for Level 1 investments that have an acquisition cost of over $100 million and IT investments with a life cycle cost of over $200 million.

—*Joint Requirements Council (JRC).*—The JRC provides decision authority for Level 2 investments that have an acquisition cost between $50 million and $100 million, and IT investments with a life cycle cost between $100 million and $200 million.

—*Enterprise Architecture Board (EAB).*—The EAB conducts a full review of Level 3 IT investments with an acquisition cost between $5 million and $50 million, and a life cycle cost between $20 million and $100 million and conducts a limited review of Level 4 IT investments (investments with an acquisition cost below $5 million and a life cycle cost below $20 million). The EAB operates within the OCIO and ensures the existence of an effective IT governance process in accordance with DHS architecture principles. As part of its overall governance strategy, the EAB conducts milestone reviews of investment initiatives to help manage architectural alignment within DHS and serve as the conduit for receiving, analyzing, and disseminating information. This process also supports the DHS CPIC (Capital Planning and Investment Control), acquisition, and budget processes, and serves to identify, evaluate, select, align, and approve investments, technologies, and policies for use in DHS.

MEETING WITH UNIONS

Question. During your confirmation hearing on February 2, 2005, you testified that you would meet with the representatives of the various union members working in the Department. Have you met with the unions?

Answer. Yes. In April, I met with the President of the National Treasury Employees Union (NTEU) and the President of the American Federation of Government Employees (AFGE). These are the two largest unions represented in DHS, and the only two with national consultation rights at the Department.

HEARINGS ON THE PATRIOT ACT

Question. The PATRIOT Act was enacted in haste, with minimal debate, in a time of crisis.

Legislation called the SAFE Act has been introduced by Senators Feingold, Craig, Durbin and others to modify certain provisions of the PATRIOT Act. While I support review of the provisions referenced in the SAFE Act, I would prefer that all provisions of the law be subject to examination in hearings held by all relevant committees of jurisdiction in the House and Senate. This law was never subject to substantial debate. In prior meetings with you, you have assured me that you would support hearings on the Patriot Act.

Do you continue to support broad ranging hearings to examine, in depth, the provisions of the PATRIOT Act?

Answer. The USA PATRIOT Act provides invaluable tools for protecting Americans from terrorist attacks while safeguarding civil liberties and preserving the important role of congressional and judicial oversight. The USA PATRIOT Act has been the subject of numerous hearings in the Congress. I am committed to working with Congress on all issues that relate to the Department, including matters, like the USA PATRIOT Act, that are crucial to terrorism prevention.

INFORMATION CONCERNING THE PATRIOT ACT

Question. As you know, when the PATRIOT Act was enacted, the Congress included sunsets on certain surveillance powers so the Congress could evaluate how those powers had been used before deciding wether to extend them or make them permanent. Some of those provisions scheduled to expire at the end of this year are not controversial. Other provisions are controversial, and some that are not even subject to sunset have been criticized for infringing on the privacy rights and civil liberties of law-abiding American citizens.

Are you committed to working with the Congress to ensure that we have the information we need from the Administration and the Department of Homeland Security in particular, so the Congress may make an informed decision about whether to renew those provisions that will expire at the end of this year or make other changes to the PATRIOT Act?

Answer. I am committed to ensuring that the Department continues to provide Congress with the appropriate information it needs.

CONSULTING WITH CONGRESS

Question. Attorney General Ashcroft engaged in minimal consultation with the Congress and members on both sides of the aisle on the PATRIOT Act and other key pieces of legislation considered in the wake of 9/11. A full draft bill, known as PATRIOT II, became public before any discussions with interested Members of Congress had taken place, and while the proposed bill was later disavowed as merely a draft, many of the proposals contained in it were subsequently included in other Administration proposals.

Now that you have been confirmed, will you continue to consult closely with Congress and Members on both sides of the aisle before rolling out new legislative proposals to expand Federal law enforcement, surveillance, and other powers that might curtail constitutional rights and protections?

Answer. I will continue to engage actively in the consultation process as we seek to offer new programs and legislative proposals.

Question. What actions are you taking in your role as head of the Department of Homeland Security to ensure that such consultation occurs?

Answer. I have conveyed to the DHS Senior Leadership and the appropriate offices within the Department of the importance of consulting with Congress and keeping Members informed of programs, policy, and operational activities within the Department. My expectation is that they will do so in a timely fashion.

SECURE FLIGHT

Question. On March 28, 2005, the Government Accountability Office (GAO) released a report entitled, "Secure Flight Development and Testing Under Way, but Risks Should be Managed as System Is Further Developed". The GAO was mandated to do this report by the fiscal year 2005 Homeland Security Appropriations Act. In essence, the report found that Secure Flight is not ready for primetime. Only one of the ten specific aspects of the development and implementation of Secure Flight has been met.

Mr. Secretary, I want to make the skies safer for all passengers who fly on commercial aircraft. But I also want to ensure that those individuals who fly have their legitimate privacy rights and civil liberties protected. And I want to ensure that whatever pre-screening system is developed is safe from abuse by outside or unauthorized entities. My main concern with Secure Flight—and its predecessors—is that I have not yet been convinced that these protections are in place. Indeed, the GAO has not yet been convinced either. Four of the ten areas the Congress mandated the GAO review are specifically focused on privacy, safety and redress. The best that the GAO can say about the status of these items is that they are "under way".

It is not yet clear that the new Secure Flight program will create a redress process for passengers to correct erroneous information, nor is it clear that it will include security measures to protect the system from unauthorized access.

Over $130 million and more than 3 years have been spent to date on Secure Flight and its predecessors. I understand your plan is to begin initial testing of this program late this summer using passenger data from two airlines. If in April 2005 the best that can be said of the program is that it is "under way", what will be the likelihood that Secure Flight will truly be "under way" in August 2005?

Answer. As we have stated, TSA intends to have Secure Flight underway later in 2005. At the request of the air carriers, TSA shifted its planned August launch date to September to account for the busy Labor Day holiday travel weekend. In addition, TSA made further adjustments to the implementation plan for Secure Flight to ensure that all regulatory and privacy documents comply with all applicable statutes and guidelines, as well as airline requests regarding technical guidance. In addition, the decision not to include commercial data in the initial rollout of Secure Flight caused further adjustments in the schedule, as did the ongoing uncertainty regarding the program's budget for fiscal year 2006. Under the revised implementation schedule, TSA expects to be in compliance with the requirement of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to implement passenger prescreening within 180 days of completion of testing.

Question. Mr. Secretary, can you commit to us that Secure Flight will not be deployed until all ten of these areas of concern are addressed?

Answer. TSA is working to meet the deadline in the IRTPA to begin to assume the watch list screening function from air carriers. As we move forward, TSA is continuing to cooperate with GAO to address the outstanding policy and operational items the agency is required to resolve under the Homeland Security Appropriations Act, 2005 (Public Law 108–334), prior to implementation. TSA will show that it has

addressed those items, as well as each of the additional GAO recommendations in its March 2005 report, prior to deployment of the program.

Question. In recent weeks, data storage systems for major companies which track and store commercial data on individual citizens have been compromised. Both ChoicePoint and LexisNexis have admitted that their databases have been accessed by unauthorized, outside entities—potentially exposing hundreds of thousands of Americans to identity theft. I have long been concerned about the privacy implications for citizens by the possible use of commercial databases for passenger screening activities. These unauthorized intrusions by outside hackers and other unscrupulous individuals only serve to enhance my concerns. The GAO has noted that Secure Flight's system safeguards and other protections from unauthorized access have not yet been developed nor tested. However, I understand that the use of commercial databases, such as these, remain under consideration for the purpose of verifying a potential traveler's identity.

Given these recent incidents, are you reconsidering the use of commercial databases?

Answer. TSA conducted a very limited test to determine whether the use of commercial data could improve the effectiveness of the watch list comparisons undertaken in the Secure Flight program as well as to assist with the identification of passenger information that is incorrect or inaccurate.

In the Homeland Security Appropriations Act, 2005 (Public Law 108–334, Section 522(d)), Congress mandated that prior to commercial data testing, TSA would be required to develop measures to assess the impact of using commercial data on aviation security, and that the GAO is to review those measures. TSA is complying with all Congressional requests on this issue and the GAO will continue to evaluate TSA's development of performance measures throughout the test phases.

TSA's testing of the use of commercial data is governed by privacy and data security protections, including strict prohibitions on the use of any passenger information provided by commercial data sources. TSA will not incorporate the use of commercial data into Secure Flight unless testing confirms that:

—it enhances security;

—it does not result in inappropriate differences in treatment of any category of persons; and

—robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain wrongful access to or use passenger personal information inappropriately.

TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Results of the testing, the comparisons of Passenger Name Record (PNR) information against names in the Terrorist Screening Database and the use of commercial data, will be as publicly transparent as possible without compromising national security. Testing and eventual implementation will be governed by strict privacy protections including passenger redress procedures, data security mechanisms, and limitations on use.

Question. What can be done to ensure the security of these databases and the integrity of the system?

Answer. TSA conducted a very limited test to determine whether the use of commercial data could improve the effectiveness of the watch list comparisons undertaken in the Secure Flight program as well as to assist with the identification of passenger information that is incorrect or inaccurate.

TSA's testing of the use of commercial data is governed by privacy and data security protections, including strict prohibitions on the use of any passenger information provided by commercial data sources. TSA will not incorporate the use of commercial data into Secure Flight unless testing confirms that:

—it enhances security;

—it does not result in inappropriate differences in treatment of any category of persons; and

—robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain wrongful access to or use passenger personal information inappropriately.

TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Results of the testing, the comparisons of PNR information against names in the Terrorist Screening Database and the use of commercial data, will be as publicly

transparent as possible without compromising national security. Testing has been governed by strict privacy protections including data security mechanisms, and limitations on use. Secure Flight has a written data control policy for this very purpose. All personnel who handle passenger data are required to sign a Non Disclosure Agreement (NDA) specific to the Secure Flight program and must successfully complete a privacy training course. Accountability for data is accomplished by assigning a control number to each disk, tape, or document on which the data is stored. In addition, a Chain of Custody process is in place to record and track data transfers by hand receipt. Finally, stand alone Government Furnished Equipment (GFE) has been identified to be used on this project. Authorization to load/install/read any PNR data is restricted to GFE designated and documented to process PNR data, and none of those machines is capable of transmitting data outside of the facility.

The Commercial Data Test also required the contractor to comply with the security requirements, regulations, and privacy protections for all records used, accessed, or contacted, as well as the data handling procedures in the Security Standard Operating Procedures and the Data Security and Control Policy. The contractor is required to comply with security requirements to maintain their Secure Facility Clearance.

Finally, the Secure Flight system will be subject to certification and accreditation prior to achieving Authority to Operate (ATO) in early fall 2005. TSA and DHS Chief Information Security Officers require all information and system security is in working order prior to ATO of the initial operating capability with initial air carriers.

SECURE FLIGHT—MOVEMENT TO SCO

Question. What impact will moving the operation of Secure Flight to the proposed Screening and Credentialing Operations office have on its implementation?

Answer. We support the concept of a Screening Coordination and Operations (SCO) Office, and requested, through the 2SR process, recommendations to best meet the goals of the office. Consistent with the 9–11 commission recommendations, HSPD–11 and HSPD–12, the SCO office would support the development of a more unified, comprehensive and efficient system for the screening, credentialing, and redress for passengers, while leveraging and optimizing investments in screening systems and tools. The SCO would be supported by a management approach that would lead to harmonized IT architecture, uniform redress, and provision of coordinated or shared services such as card production, biometric/biographic databases, and global enrollment systems/processes that adhere to standards set by DHS with close linkage to policy decisions and overall information technology enterprise architectures. The SCO office would also ensure a consistent approach also for outreach in the areas of privacy, civil rights, and helping to ensure coordinated R&D efforts. DHS plans to set up the SCO office in fiscal year 2006.

Question. Do you have concerns that further rearranging the organizational chart will further slow the development and operation of Secure Flight?

Answer. The exact roles, responsibilities, and composition of the SCO are currently under review and further definition and refinement of the SCO concept will be developed based on that review. An implementation and transition plan for the SCO will also be developed based on that review.

Question. If it is moved, who will actually maintain and operate the system—the SCO or TSA?

Answer. The exact roles, responsibilities, and composition of the SCO are currently under review and further definition and refinement of the SCO concept will be developed based on that review.

Question. Have you experienced any delays in receiving timely security information from the Terrorist Screening Center (which is run by the FBI) for Secure Flight or your other screening programs?

Answer. No, TSA has not.

SECURE FLIGHT AND PRIVACY

Question. Mr. Secretary, I'm concerned about reports from February and the end of March in which TSA officials, including a TSA spokesperson, declared that Secure Flight will be implemented in August with two airlines nationwide. That implementation would appear to violate the law as mandated by § 522 of the fiscal year 2005 Department of Homeland Security Appropriations Act that prohibits the spending of any sums appropriated on other than a test basis for Secure Flight unless and until the GAO certifies to Congress that 10 criteria are met. Is that implementation with two airlines scheduled to end at a certain time so that it can be evaluated?

Answer. TSA is proceeding with demonstrating initial operating capability for Secure Flight later this year. This timeframe is consistent with the requirements laid out in IRTPA. In addition, TSA intends to provide proof that each of the ten identified areas of concern and the six GAO recommendations have been addressed before the planned initial operating capability is implemented. Evaluations of the performance of the program with the launch carriers will be conducted prior to the program integrating additional airlines. A specific timeline is still under development to ensure that all appropriate evaluation takes place.

Question. Will the passengers flying those two airlines come late August be able to distinguish between a test run of Secure Flight and the real thing?

Answer. The passengers flying on the initial airlines will not be able to distinguish between the test run of Secure Flight and the "real thing." During the first phase of implementation, the carriers will continue their normal vetting activities and a parallel operations activity will be running in conjunction with TSA to confirm the effective processing of related data without disruption to ongoing business operations. Once the systems have performed in parallel for a period of time, and the acceptable stabilization has occurred, TSA will work with the carriers to ensure a smooth transition in taking over from them the full watch list vetting function.

Question. Do you anticipate that the Secure Flight program will, when finally implemented, use private companies to aggregate data on passengers and perform verification checks?

Answer. This is undetermined. TSA conducted a very limited test to determine whether the use of commercial data could improve the effectiveness of the watch list comparisons undertaken in the Secure Flight program as well as to assist with the identification of passenger information that is incorrect or inaccurate.

In the Homeland Security Appropriations Act, 2005 (Public Law 108–334, Section 522(d)), Congress mandated that prior to commercial data testing, TSA would be required to develop measures to assess the impact of using commercial data on aviation security, and that GAO is to review those measures. TSA is complying with all Congressional requests on this issue; GAO will continue to evaluate TSA's development of performance measures throughout the test phases. The limited commercial data testing concluded in July 2005.

TSA's testing of the use of commercial data is governed by strict privacy and data security protections, including strict prohibitions on the use of any passenger-provided information by commercial data providers. TSA will not incorporate the use of commercial data into Secure Flight unless testing confirms that:

—it enhances security;

—it does not result in inappropriate differences in treatment of any category of persons; and

—robust data security safeguards and privacy protections can be put in place to ensure that commercial entities do not gain inappropriate access to or use passenger personal information inappropriately.

TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Results of the testing, both of the comparisons of PNR information against names in the Terrorist Screening Database and the use of commercial data, will be as publicly transparent as possible without compromising national security. Testing and eventual implementation will be governed by strict privacy protections including passenger redress procedures, data security mechanisms, and limitations on use.

Question. How many companies could provide the data broker and data aggregation function to accomplish Secure Flight passenger verification?

Answer. This is undetermined at this point. TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Question. Will you examine whether the private companies bidding for this work have had data spills, or data breaches caused by identity thieves?

Answer. This is undetermined at this point. However, as with all contracts, TSA would set standards, establish program priorities and direction, establish policies, make program decisions, and monitor contractor performance. TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Question. What penalties will the Secretary impose on the company DHS and TSA eventually contracts with to perform passenger verification for Secure Flight if that company fails to properly safeguard data transferred as part of Secure Flight?

Answer. This is undetermined at this point. However, as with all contracts, TSA would set standards, establish program priorities and direction, establish policies, make program decisions, and monitor contractor performance. TSA will not incorporate the use of commercial data into the Secure Flight program prior to the completion of testing, assessment of results, final approval by the Administration, and publication of a new System of Records Notice and Privacy Impact Assessment announcing the use of commercial data.

Question. I am concerned about recent GAO reports that show a lack of progress regarding establishing a transparent, concrete and workable system of due process and redress for passengers wrongly selected for extra scrutiny who might miss a flight and those who are wrongly put on a no fly list.

Mr. Secretary, please share with us what efforts you will take to ensure that the government's own watch lists and databases used for Secure Flight contain accurate information about would-be passengers.

Answer. U.S. Government intelligence and law enforcement agencies collect, analyze, and evaluate data used to nominate subjects to the No-Fly List. Intelligence analysts and law enforcement officers within these organizations carefully review nominations based on the No-Fly List criteria and thoroughly evaluate the information during each step of the process. Watch List nominations often contain classified and/or sensitive law enforcement investigative information. Nominations that meet the established criteria are forwarded to the National Counterterrorism Center (NCTC) and the Terrorist Screening Center (TSC) for inclusion in the TSC Data Base (TSDB) and for addition to the No-Fly List. Time sensitive nominations may be routed directly to the TSC if required.

If it is determined that a person on the No-Fly List should no longer be identified as a No-Fly subject, they will be removed from the list. If additional intelligence data is developed or a subject has been interviewed by U.S. Government officials and deemed no longer a threat, an official request for removal must be submitted to the agency that placed the individual on the list. The original nominating agency will evaluate the data and determine whether the person stays on or is removed from the No-Fly List. The nominating agency will then make a formal request through the nomination chain requesting that the person be removed from the No-Fly List. In some cases, a review of the derogatory information associated with a No-Fly nomination may result in the subject being downgraded to the TSA Selectee List.

The TSA Office of Transportation Security Redress is developing a redress process that will address any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have been erroneously placed on the watch lists to undergo a case review. The Office of Transportation Security Redress will work to ensure that passengers erroneously placed on the watch lists are in fact provided relief. The redress process will be coordinated with other DHS redress processes as appropriate.

TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due to the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

However, this clearance process will not remove a name from the watch lists. Instead, this process distinguishes legitimate passengers from persons who are on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Following TSA-required identity verification procedures, airline personnel can then quickly determine that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction after the redress and appeals process within TSA has been exhausted.

Question. And tell us what concrete redress policies you envision for passengers wrongly detained for additional screening who might miss a flight or those wrongly placed on a no-fly list.

Answer. The TSA Office of Transportation Security Redress is developing a redress process that will address any situation where passengers believe they have been unfairly or incorrectly singled out for additional screening under the future Secure Flight program. This process will also allow passengers who feel they have been erroneously placed on the watch lists to undergo a case review. TSA will work with the nominating agency to review the derogatory information. The redress process will be coordinated with other DHS redress processes as appropriate.

TSA has developed and implemented a clearance protocol for persons who are flagged for additional screening due the similarity of their names to those of individuals who are appropriately on the watch lists. A passenger may initiate the clearance protocol by submitting a completed Passenger Identity Verification Form to TSA headquarters. TSA will review the submission and reach a determination of whether these procedures may aid in expediting a passenger's check-in process for a boarding pass. The Passenger Identify Verification Form, as well as other information, has been posted on TSA's public website at the following web address: http://www.tsa.gov/public/display?theme=157&content=09000519800fb8af

It is important to keep in mind that this clearance process will not remove a name from the watch lists. Instead, this process distinguishes passengers from persons who are in fact on the watch lists by placing their names and identifying information in a cleared portion of the lists. This information is transmitted to the airlines. Airline personnel can then more quickly determine when implementing TSA-required identity verification procedures that these passengers are not the person of interest whose name is actually on the watch lists.

In addition, an individual may seek to challenge his or her inclusion on a watch list in a court of competent jurisdiction, after the redress and appeals process within TSA has been exhausted.

US VISIT: WHEN WILL WE HAVE A REAL "EXIT" COMPONENT?

Question. The former DHS Under Secretary, Asa Hutchison, announced with great fanfare meeting the December 31, 2004 deadline to have the foreign visitor visa entry-exit system, known as US VISIT, up and running at the 50 largest land-border ports of entry. This is a positive accomplishment and I am pleased that the Department has taken seriously our mutual interest in knowing who is entering this country and in keeping out those who should not be allowed entrance.

However, I remain concerned that very few taxpayers know that while we may know who is entering the United States at our airports, seaports, and some land border ports, we continue NOT to know who is exiting the United States. That's right—there is almost no "exit' component to the US VISIT system—a system which used to be called "entry-exit". We have spent hundreds of millions of dollars on this system—and another $390 million is requested for US VISIT in the President's fiscal year 2006 budget, and yet we still are not able to capture data on which visitors are exiting the country.

How can we know if someone has overstayed their permitted time in this country if we do not know that they have left?

Answer. US VISIT is exploring different departure confirmation alternatives where biometrics are collected on exit, in addition to the biographic information, at 12 air and 2 sea port pilot locations. After evaluating these exit procedures, DHS will select the most effective process(es) and technologies to implement at airports and seaports nation-wide.

Currently the US VISIT system collects both biographic and biometric data on eligible (nonimmigrant) alien arrivals and departures and stores the data in the Arrival Departure Information System (ADIS).

—Biographic data is primarily collected through the submission of passenger manifests by the transportation carriers, with additional arrival and departure information collected by officers at U.S. ports-of-entry.

—Biometric data (digital fingerscans and photographs) are collected at consular posts during visa interviews, at U.S. air and sea ports-of-entry during admission, and at a limited number of pilot locations at air and sea ports during departure.

—US VISIT analyzes the data in ADIS to prepare the Annual Report on Integrated Entry and Exit Data System, as required by the Data Management Improvement Act of 2000 (Public Law 106–215) and the Visa Waiver Permanent Program Act (Public Law 106–396). The report is due on December 31 each year. The report for 2004 was transmitted to the Hill on August 19, 2005.

—During the last 3 months of the reporting period ending in September 2004, the system consistently matched 90 percent of exit records to entry records using biometrics due to the increased number of visitors enrolled in US VISIT at the

time of admission. The system successfully matched approximately 10 percent more exit records than when using biographic data alone.

—US VISIT then analyzes those remaining records to determine if stays were legally extended, there were approved changes in status, or information existing in other systems that would indicate that the individual did not overstay.

—Once US VISIT reviews all the information, those who are "confirmed overstays" are referred to ICE's Compliance Enforcement Unit for further vetting. Based on the outcome of its analysis, ICE may refer unresolved cases to the field for investigation. From January 2004 through August 2005, ICE has arrested almost 70 individuals based on overstay information provided by US VISIT.

—DHS also will leverage new technology in the land environment to capture information about and departures. Our first proof of concept using this new technology, radio frequency identification (RFID), began August 4, 2005, at three land border ports of entry along the Northern and two along the Southern borders. This technology can detect a visitor at a distance and provide primary inspection officers with entry information as well as provide a mechanism for an accurate and timely record of exits. The proof of concept testing at the ports of Nogales East and Nogales West in Arizona, Alexandria Bay in New York, and the Pacific Highway and Peace Arch in Washington will continue through 2006.

Question. What are the threats from not knowing who left?

Answer. These threats are difficult to measure. Where we develop a lead that someone is associated with a terrorist group after that person has entered the country ICE coordinates its investigative activity with necessary entities to take appropriate action. In addition, one of the purposes of the Immigration and Nationality Act (INA) is to exclude and remove criminals, terrorists, drug traffickers, and those who would work and live in United States illegally, from the United States. Individuals who overstay their visas contribute to the denigration of the integrity of our immigration system—that is why US VISIT works with ICE to locate and apprehend these immigration violators.

Question. When will we have a robust "exit" capability at our airports and at our land borders?

Answer. US VISIT is exploring different biometric departure confirmation alternatives at 12 airports and two seaports. The exit pilots require foreign visitors to check out at an exit station or with a US VISIT exit attendant at the departure gate at the port. After evaluating these exit procedures, DHS will select the most effective process(es) and technologies to implement at airports and seaports nationwide.

Question. How much more will this cost and when will this system be completed?

Answer. The fiscal year 2005 investment includes resources to modernize our immigration and border management systems and provide greater interoperability for immigration and border management data. In fiscal year 2005, we will increase interoperability technology and introduce basic common service-oriented architecture functionality to enable delivery of expanded person-centric view capabilities. We are currently developing the business requirements for the first phase of this strategy.

The fiscal year 2006 request includes resources to improve our immigration and border managements systems, as well as the continued deployment of US VISIT at our land borders. The fiscal year 2006 request includes operation and maintenance of current and 2005 investments, including: initial implementation of the entry and exit solution at air, sea and land ports of entry (POEs); implementation and integration of border technology to the busiest land POEs; and deployment of biometric travel document readers at air, sea, and land POEs.

US VISIT

Question. In the Immigration and Customs Enforcement (ICE) reprogramming request submitted to Congress on March 11, 2005, the Department offered up as a "bill payer" a portion of the US VISIT "management reserve." The US VISIT program office had vociferously advocated for this reserve. The Department suggested that this reserve could be reduced by $17 million to meet the ICE funding shortfalls which had been known by the Department for sometime.

Does this mean that the US VISIT management reserve is a lower priority to the Department? Will we see this reflected in the next US VISIT spend plan we expect to see regarding the fiscal year 2006 funds?

Answer. All components within DHS were asked to review their budgets to determine if they could help address ICE funding needs. Management reserve within US VISIT exists to address unforeseen funding issues as they arise. This helps reduce

program risk. Because of the nature of the purpose of management reserve, it is difficult to determine with certainty how much is needed in any given year. To reduce programmatic risk on ICE programs, it was appropriate to propose to accept temporary higher risk for US VISIT. However, a normal level of management reserve must be an integral part of the program into the future.

The recently enacted fiscal year 2005 supplemental for ICE eliminated the need to reprogram funding from US VISIT for this purpose.

TWIC PROGRAM—WHY THE DELAY?

Question. During his confirmation hearing before the Senate Homeland Security and Governmental Affairs Committee on March 8, 2005, then Deputy Secretary-nominee, Michael Jackson, said he did not understand why it was taking so long to get the Transportation Worker Identification Credential (TWIC) program up and running. He said, "It's not rocket science." A number of states, notably Florida, have already moved forward with their own credentialing programs for their State workers. Mr. Secretary, if this program is not "rocket science", what is causing the delay? Congress has provided upwards of $65 million towards the program, pilot projects are underway, and thousands of workers are waiting. Why the delay? Is this delay the result of resource-constraints, policy decisions, privacy protections (or lack of clarification of privacy protections) decisions, some combination all of these, or something else?

Answer. TSA acknowledges that the TWIC prototype has proceeded slower than expected. Technical and contractual issues have delayed rollout of the final TWIC card model and installation of final version biometric access control readers. Those issues are now solved. Enrollments and card production are ramping up at East and West Coast sites. The Florida rollout has been slowed as the State of Florida's team worked to resolve issues unique to Florida due to the need to comply fully with the Florida Uniform Port Access Credential (FUPAC) Act. Working with both State personnel and the prototype contractor the program has been successful in addressing and solving these problems. The ability to discover and resolve problems during the prototype phase rather than during implementation has been a welcome and valuable result and will benefit the program as it moves forward.

The TWIC Program achieved initial operating capability (IOC) for each region on November 17, 2004. IOC was defined as having functional enrollment capability and at least one operational TWIC reader at one or more sites within the region. Presently, TWIC is in Phase III-Prototype whereby TSA is evaluating a full range of business processes, policies and requirements for an end-to-end solution that includes sponsorship, claimed identity verification, criminal history records checks (in the State of FL only) and card production, personalization, and issuance as well as revocation. Once Phase III-Prototype is complete, TSA will conduct further analysis and make recommendations regarding the nature and scope of Phase IV-Implementation.

EXPEDITED TRAVELER EXPANDING OVERSEAS

Question. The Department announced the creation of pilot expedited traveler program at Schipol Airport in Amsterdam, yet there has been no decision made on expanding or making permanent the limited pilot tests of the Registered Traveler program here in the United States. Why is there a delay with expanding the domestic Registered Traveler program?

Answer. While both programs enhance the security of civilian aviation, the two programs serve different purposes. The International Register Traveler Program is intended to enhance the already-existing requirement that CBP inspect and interview travelers seeking to enter the United States, and the program enhances CBP's ability to make admissibility decisions by separating out low-risk travelers. It builds on legacy trusted traveler programs—e.g., SENTRI, NEXUS, FAST, INS PASS. The domestic registered traveler program, by contrast, is a pilot program to improve the aviation security screening process by helping TSA align screeners and resources with potential risks.

Through a series of concurrent stand-alone pilots, TSA has been aggressively testing the Registered Traveler (RT) concept of running threat assessment and identity verification checks on eligible volunteers in order to provide them with an expedited clearance through security checkpoints. TSA is currently running pilot programs at five Federally managed sites (Minneapolis, Los Angeles, Houston, Boston, and Washington, D.C.), which are scheduled to be completed in September 2005. TSA has also worked with the Greater Orlando Aviation Authority (GOAA) to launch a pilot at Orlando International Airport that is assessing the feasibility of incorporating a private sector component into the RT concept.

Results of these pilots will be analyzed to determine the program's effect on security and service, enabling the Department to make decisions about full scale implementation of RT. Any timeline and deployment schedule for implementing RT beyond the pilot stage will be linked to the Department's decision.

Question. If we're not sure the domestic program is going to work—or how exactly it should be structured—why are you starting an international version at this time?

Answer. While both programs enhance the security of civilian aviation, the two programs serve different purposes. The International Register Traveler Program is intended to enhance the already-existing requirement that CBP inspect and interview travelers seeking to enter the United States, and the program enhances CBP's ability to make admissibility decisions by separating out low-risk travelers. It builds on legacy trusted traveler programs—e.g., SENTRI, NEXUS, FAST, INS PASS. The domestic registered traveler program, by contrast, is a pilot program to improve the aviation security screening process by helping TSA align screeners and resources with potential risks.

Through a series of concurrent stand-alone pilots, TSA has been aggressively testing the Registered Traveler (RT) concept of running threat assessment and identity verification checks on eligible volunteers in order to provide them with an expedited clearance through security checkpoints. TSA has run pilot programs at five Federally managed sites (Minneapolis, Los Angeles, Houston, Boston, and Washington, D.C.), which are scheduled to be completed in September 2005. TSA has also worked with the Greater Orlando Aviation Authority (GOAA) to launch a pilot at Orlando International Airport that is assessing the feasibility of incorporating a private sector component into the RT concept.

Results of these pilots are being analyzed to determine the program's effect on security and service, enabling the Department to make decisions about full scale implementation of RT. Any timeline and deployment schedule for implementing RT beyond the pilot stage will be linked to the Department's decision.

LACK OF FUNDING FOR BORDER SECURITY

Question. During the hearing, you stated that the President's budget for fiscal year 2006 both hires 210 new Border Patrol agents, hires more immigration investigators and provides 1,920 new detention bed spaces and, at the same time, provides sufficient funds to backfill and hire the positions that were lost during the current fiscal year.

Are you guaranteeing that the budget request hires both all fiscal year 2005 attrited Border Patrol positions and 210 new Border Patrol agents?

Answer. The fiscal year 2005 Emergency Supplemental provides funding for 500 additional Border Patrol agents. CBP has until the end of fiscal year 2006 to fill these positions. However, CBP plans to hire these positions aggressively. For fiscal year 2005, CBP will backfill its fiscal year 2005 attrited positions and hire approximately 400 (of the 500) additional agents.

For fiscal year 2006, the President's Budget requests 210 additional Border Patrol agents. Both House and Senate Appropriations bills add 790 Border Patrol agents on top of this (for a total of 1,000). If enacted, CBP would hire these positions and backfill estimated attrition (approximately 600 positions).

With that said, the total impact of the fiscal year 2005 Supplemental and the anticipated fiscal year 2006 budget will result in 1,500 new Border Patrol agents by the end of fiscal year 2006. CBP will also hire for the backfill of attrition. CBP has the capacity to hire and train this level.

With respect to ICE, the fiscal year 2006 President's Budget, when combined with projected carryover balances from the fiscal year 2005 Emergency Supplemental, contains sufficient funding to support 376 fiscal year 2005 attrition hires. In addition, the fiscal year 2006 President's Budget includes an increase of $90 million to support 1,920 beds.

Question. And at what point in fiscal year 2006 will the Border Patrol have hired and trained the same staffing level at the start of fiscal year 2005 positions, plus the 210 new agents?

Answer. CBP ended fiscal year 2004 with 10,817 Border Patrol (BP) agents. For fiscal year 2005, CBP plans to maintain that staffing level as well as beginning to add the 500 new agent positions provided in the fiscal year 2005 supplemental. For fiscal year 2006, CBP plans to add the 210 new agents in the President's Budget and replace all attrition positions. Hiring for the additional BP agents is a high priority.

BORDER SECURITY

Question. The Heritage Foundation's December 13, 2004 report recommends that the Department "conduct a national assessment of the resources required for effective border security." Is this recommendation a part of your comprehensive review of the Department and its priorities?

Answer. The Department has been working aggressively outside of the Second Stage Review process to assess our long-term border needs, including the resources needed to secure substantial improvement in control of our borders. Complimentary Second Stage Review efforts examined needs in such areas as cargo security and passenger screening. The Department also is developing a plan for an independent, outside entity to examine border resource needs. All of our efforts will coalesce into the development of a long-term border security and immigration reform plan.

IMPACT OF REAL ID ON BACKLOG REDUCTION/WORKLOAD

Question. The House attached Rep. Sensenbrenner's REAL ID immigration bill (H.R. 418) to the Emergency Iraqi War Supplemental. This bill includes many of the provisions in the original House draft of the Intelligence Reform and Terrorism Prevention Act.

Unlike some rhetorical Bush Administration amnesty, the specifics of this legislation are known. The Administration supports the REAL ID legislation.

If the conferees decide to include the provisions of this bill in the Supplemental, what impact would it have on Citizenship and Immigration Service's abilities to meet its backlog reduction goals and what resources would be required to implement the Act?

Answer. Based upon our review, the Real ID legislation should have no impact on the backlog elimination plan. The additional fee revenues as a result of this legislation ensure the timely processing of these cases.

The verification and adjudications functions of USCIS are organizationally separate. The verification workload is handled by Immigration Status Verifiers (ISVs) in the USCIS Records program, who are dedicated and specially trained for that function. USCIS does not intend to divert adjudications resources to implement the REAL ID Act. Therefore, backlog elimination goals will not be impacted.

PASSPORT PRIVACY

Question. As the State Department is looking into the issue of possibly embedding personal data in the next generation of U.S. passports, what if any discussion has the Department's Privacy Officer had with State Department officials about the protection of the privacy of U.S. citizens?

Answer. The Chief Privacy Officer for DHS has a very good working relationship with officials from the Department of State on matters of mutual concern, including lost and stolen passports and appropriate privacy notices for international travelers. While the Privacy Officer has made her views known to the State Department on numerous privacy matters, the precise question of how to protect personal information in the next generation of U.S. passports is one that is being worked on primarily by the Department of State, which has the lead authority for matters pertaining to passports. Of course, the DHS Chief Privacy Officer will work collaboratively with the State Department to ensure that implementation of any decisions protect the privacy of U.S. citizen's information.

CARGO CONTAINER SECURITY

Question. The conference report accompanying the fiscal year 2005 Appropriations Act notes that over $200 million has been spent over the past 3 years on various projects designed to secure cargo containers entering this country. It also calls on the Under Secretary for Border and Transportation Security to report to the Congress no later than February 8, 2005 on which DHS entity will have primary responsibility for cargo container security and the setting of shipping industry standards. To date we have not yet received that report. When can we expect to see it?

Answer. This report was submitted to Congress on May 31, 2005.

Question. Are funds included in the President's budget request to achieve this goal?

Answer. The President's fiscal year 2006 Budget includes $138 million for the Container Security Program.

SUPPLY CHAIN AND CONTAINER SECURITY

Question. We received part one of the Supply Chain and Container Security report required by House Report 108–541. It states that the Container Security Initiative

Division in headquarters "is staffed with a majority of CBP employees and a small number of ICE Special Agents.

Please provide the total number of the CSI Division headquarters staff and the number of those who are ICE Special Agents. Also, at which—if any—of the overseas CSI ports do we have both an ICE and a CBP attaché?

Answer. The Container Security Initiative (CSI) Division headquarters staff consists of 52 full time employees, four of which are ICE Special Agents. At this time, there are no CSI ports with both an ICE and a CBP Attaché.

MERGING CBP AND ICE

Question. You currently are conducting a "top to bottom" review of the Department, its structure, and its operations. Recent reports, including a December 13, 2004 Heritage Foundation report, bemoan the artificial division of Customs and immigration inspectors from Customs and immigration agents and recommend that CBP and ICE be merged. What is the status of the Department's discussion on these recommendations? When will the Congress learn of your intentions, if any, in this regard?

Answer. We are not merging ICE and CBP; however, we do see the need to ensure that these organizations coordinate better. We will continue to work closely with the leaders of ICE and CBP to improve cooperation and coordination between these agencies. In deciding to not merge the two agencies, we considered view points from a variety of sources, including think tanks, as well as the Department's Inspector General, Members of Congress, and other valuable stakeholders.

As you know, the Department looked at a variety of organizational issues as part of the Second-Stage Review process, which helped clarify where the Department needs to be organizationally to ensure effective implementation of our critical missions. We considered whether ICE should remain a stand-alone entity, and decided that it should. We believe it's in the Department's best near and long-term interest that ICE not be merged with another component, CBP in particular. To reach this decision, we focused on the operational mission needs of both CBP and ICE, not on the near-term management challenges. I take seriously the challenges the Department has faced concerning ICE and appreciate the difficult but necessary choices Congress has made in providing new funding to address its needs. I am confident, however, that ICE has made substantial improvements in financial management this year. Not only have substantial new resources been provided, but a new management team is taking shape.

IDENT/IAFIS

Question. The integration of the fingerprint databases created, maintained, and used by the Department of Homeland Security and the FBI—among other Federal agencies—continues to be a priority concern for the Congress and the members of this Subcommittee. Border Patrol agents daily compare the fingerprints of illegal aliens apprehended at our borders against these databases. And Customs and Border Protection inspectors—at a growing number of ports of entry—compare the fingerprints of visa holders and others wishing to enter this country against these same databases via the US VISIT system.

That is why I was concerned about the latest Department of Justice Inspector General report on this subject. It stated that of the 118,000 visitors daily entering this country who are subject to US VISIT, an average of about 22,350 individuals are referred for secondary inspection.

According to DHS, by the end of this fiscal year, it expects to directly check only about 800 individuals each day against the full FBI fingerprint database known as the IAFIS Criminal Master File. This is just 0.7 percent of the 118,000 daily visitors. The vast majority of the visitors, 99.3 percent, will be checked only against the US VISIT watch list. These persons will not be checked directly against the full IAFIS Criminal Master File. Why is that the case? Why are so few people being run against these valuable investigative tools?

Answer. The Department continues to work closely with the Department of Justice to improve the integration and interoperability of our fingerprint databases and we have established an integrated project team. Currently, the FBI updates DHS' records with information from a variety of criminal and threat-related databases. Based on updates to the US VISIT system during the time period between January 2004 and the end of August 2005, officers have taken adverse action against more than 800 individuals during US VISIT processing on entry. In addition, integrated DHS Automated Biometric Identification System (IDENT) and FBI Integrated Automated Fingerprint Identification System (IAFIS) workstations will be deployed to all POEs with significant passenger volume, as well as to ICE locations by the end of

calendar year 2005. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

On July 13, 2005, I announced a decision that first-time visitors to the United States will be enrolled in the program by submitting ten fingerscans—a key step to achieving interoperability between IDENT/IAFIS. We have worked with the Departments of State and Justice to develop an implementation plan for the Initial Transition to 10 Print Plan which addresses interoperability as well as migration to 10 fingerscans. In addition, the capability to capture 10 fingerscans will allow us to increase accuracy for matching individuals against watch lists and previous enrollment records; improve DHS's ability to match enrollees against latent prints; and allow DHS to focus more time and attention on individuals who might be potential risks to the country.

Question. The Conference Report accompanying the fiscal year 2005 Homeland Security Appropriations Act directs the Department to fund the full cost associated to achieve real time interoperability with the US VISIT system. Yet there does not appear to be any funding in the budget to either establish real time interoperability of the DHS and Justice fingerprint databases, or an expansion of the current DHS system of capturing 2-fingerprints versus movement towards a 10-print system.

Why is there no specific funding in the budget to improve the interoperability of IDENT/IAFIS and US VISIT?

Answer. On July 13, 2005, I announced a decision that visitors to the United States will be enrolled in the US VISIT program by submitting 10 fingerscans. DHS is working with the Departments of State and Justice to develop an implementation plan that will address interoperability as well as migration to 10 fingerscans and cost estimates.

There are several different ongoing efforts to bring about interoperability between the IDENT/IAFIS systems. Integrated IDENT/IAFIS capabilities were deployed to all Border Patrol stations ahead of schedule in fiscal year 2004 and additional deployment to all POEs with significant passenger volume and ICE offices will be completed by the end of calendar year 2005. The US VISIT program will use $9.3 million of fiscal year 2005 resources to complete the deployment of IDENT/IAFIS access configuration at 115 airports, 15 seaports, and 165 land border POEs, as well as to specific ICE locations.

The fiscal year 2006 budget request includes resources for improved interoperability and the integrated project team will develop cost estimates for primary integration and development associated with IDENT/IAFIS interoperability as it develops its plan.

IDENT/IAFIS INTEGRATION

Question. In the Department's "2004 Year End Review", it is noted that the Integrated Automated Fingerprint System (IAFIS) was operational at all Border Patrol stations 3 months ahead of schedule. This is a positive first step. However, nowhere in the report does the Department discuss the progress at fully integrating the IAFIS and IDENT fingerprint databases. The statement of managers accompanying the conference report on the fiscal year 2005 Appropriations Act discusses at length the strong congressional interest having these databases fully integrated. In fact, this was a topic that generated much bipartisan discussion during one of our hearings last year. Chairman Gregg again stressed its importance during our hearing with you this year.

Integration has also been the subject of at least three Department of Justice inspector general reports.

Who in the Department has the lead on this subject?

Answer. The US VISIT Program, working closely with DHS components such as CBP and ICE, and the Departments of Justice and State, leads the efforts for full IDENT/IAFIS interoperability within the Department.

Question. What is the timeline for accomplishing this integration and how much will it cost?

Answer. DHS (US VISIT) and FBI/CJIS have established an IPT to address the policy, business requirements, and technical aspects of integrating IDENT and IAFIS. This IPT has made significant progress in resolving many of the long-standing issues originally referenced by the DOJ Office of the Inspector General. A report, describing plans for interoperability, was submitted to Congress on August 18, 2005.

Question. Are sufficient/any funds included in the President's budget request for this activity?

Answer. The Departments of Homeland Security and Justice will develop future budgets to support any necessary level of funding for IDENT/IAFIS interoperability.

VEHICLE FLEET MANAGEMENT REPORT

Question. Senate Report 108–280 required the submission by February 8, 2005 of a vehicle fleet management report. That report has yet to be submitted. It is difficult for the Congress to provide funds for new and replacement vehicles when we have little confidence that decisions to purchase these vehicles are being made in a methodical and reasoned manner. When can we expect to receive this overdue report? Also, please break out by type/category of vehicle the funds requested in the budget for new and replacement vehicles for the various CBP entities.

Answer. The requested report is now being reviewed and will be submitted to Congress as soon as possible. The type and number of vehicles to be purchased will be based on the operational priorities of the Border Patrol in fiscal year 2006.

AMO FLEET MODERNIZATION PLAN

Question. House Report 108–541 required submission of a report on the costs and benefits associated with a service life extension program of the P–3 Orion aircraft 30 days after enactment of the act. To date we have not received this report. Please provide us with this report as well as the status of Air and Marine Operations long-term procurement plan for new and replacement air and marine assets, including P–3.

Answer. A technical and operational review of responses received in reply to the CBP Request for Information (RFI) issued on February 28, 2005, has been completed. This review concluded that while there are viable alternatives to either replace or remanufacture the CBP/AMO P–3 fleet, this effort should be part of a formal acquisition process associated with CBP/AMO's overall modernization initiative. CBP's long-term modernization plan will be developed as a component of the CBP air asset integration study to be completed in the summer of fiscal year 2005.

APHIS—FOOD SAFETY INSPECTORS

Question. Since the announcement of the creation of the Department, I have been concerned that "core" missions of the various legacy agencies would get lost because of the new Department's primary focus on homeland security. One area of concern is agriculture inspection operations at our borders.

Border inspection responsibilities, including 2,500 frontline inspectors, were transferred from the Animal and Plant Health Inspection Service (APHIS) to DHS in March of 2003.

According to a recent U.S. Department of Agriculture Inspector General report, APHIS could not assure that the DHS process for agriculture inspection operations contains adequate controls to safeguard U.S. Agriculture against entry of foreign pests and disease. It also noted that there was a reported 32 percent drop in the number of pest inspections following the transfer to DHS. What is the Department doing to correct this?

Answer. The effort to bring up the number of CBP agricultural specialists to the level transferred from APHIS is a priority and CBP has made significant progress. According to the Determination Order that actually transferred personnel from APHIS, 1,872 agricultural specialists including canine were sent to DHS CBP. Of these positions, 316 were vacancies. In fiscal year 2005, the hiring of additional Agriculture Specialists is a priority. The USDA Professional Development Center (PDC), the APHIS entity responsible for training new CBP agricultural specialists, has scheduled 20 classes from May 2004 through February 2006. Seven classes have graduated as of April 22, 2005, with 203 graduates deployed to 62 POEs. It is projected that CBP will have 500 graduates by February 2006.

In addition to training more agricultural specialists, under CBP's "One Face at the Border" initiative, all CBP Officers at the POEs are used to perform the vast number of functions that CBP is charged with carrying out. In terms of agricultural inspections, CBP officers are being cross-trained, learning basic agriculture procedures for the land border, mail, cargo, maritime, and air passenger pathways to increase the value of referrals and supplement the work of the Agriculture specialists.

CBP has noticed that several positive developments have resulted in a greater level of compliance in agricultural importations. Offshore mitigation strategies by APHIS to minimize the number of pests even reaching the United States are working. CBP, in conjunction with APHIS, has entered into several programs, such as a targeted program for imported cut flowers that decreased the number of inspections because the scientific data indicates that such commodities pose a much lower risk to American agriculture. During the same period, interceptions of prohibited animal by-products went up by 26 percent and prohibited meat and poultry by 6 percent.

In summary, as the vacancies are filled with newly trained specialists, CBP will create a sufficient workforce of agricultural specialists to target and intercept prohibited material, and report all insects found in CBP seizures. When this occurs, the interception rate will more precisely reflect the true level of CBP efforts. CBP has asked USDA to supply additional insect pest detection training at POEs based on the specific pest pathways of concern.

Question. Is the Department working with APHIS to establish a method to coordinate information regarding inspections?

Answer. DHS–CBP has been working with and coordinating with USDA–APHIS in numerous ways to synchronize and verify information and data collected about inspections. The following are some of the ways CBP and APHIS have worked together.

Joint Quality Assurance (QA) Program

—CBP and APHIS have formed a joint QA team and began conducting port reviews together.
—QA reviews will assist the Directors, Field Operations and improve our credibility among agricultural stakeholders.
—CBP's Agricultural Inspections Policy and Programs (AIPP) conducted successful Joint APHIS QA reviews at the Port of Philadelphia, December 7 and 8, 2004, and the Port of Miami, April 18–22, 2005.
—Plans and dates are being developed to conduct Joint QA reviews once a month for the remainder of fiscal year 2005.
—The QA team produces recommendations that are conveyed to CBP management for consideration and action.

Creation of selectivity criteria and rule sets for agricultural targeting

—CBP AIPP and APHIS are working together to develop rule sets for targeting and prevention of Agro/Bio Terrorism.
—Plans are in place to hire two CBP Agriculture Specialists to be assigned to the National Targeting Center (NTC).
—CBP assisted APHIS in the placement of one employee at the NTC to target and help prevent Agro/Bio Terrorism.
—CBP has engaged and included APHIS in discussions about developing selectivity criteria for agricultural products.

USDA access to CBP databases

—CBP has been instrumental in negotiating an agreement with USDA to share data and databases between the agencies.
—CBP has granted access for certain USDA offices to relevant CBP databases.
—The combination of USDA databases and CBP databases and electronic systems will add to our capability to measure agricultural risk worldwide, target, develop new rule sets, and build CBP's expertise and capacity for early threat detection.

Communications within CBP

—CBP is making efforts to redesign and improve the Agriculture Inspection section of the cbp.gov website to be an effective means of communication within CBP.
—The intranet site, cbp.net, is being redesigned to highlight joint actions and important efforts with USDA/APHIS.
—CBP uses a system of alerts and musters as well as other CBP systems to notify the ports of issues of immediate concern.

Joint Operations with USDA—Measurement Driven Special Operations (MDSO)

—Fifty joint MDSO's are proposed for the remainder of fiscal year 2005.

Management Inspection Division (MID)

—CBP used the MID to establish audit protocols that target mission critical agriculture functions.
—Planning inspections at JFK, Miami, Los Angles and Newark International Airports: International Mail, Pest Interceptions (Cargo), Pest Interceptions (PAX), Cargo Control (Agriculture), Agriculture Quarantine Inspection Monitoring (AQIM).
—Proposed MID Inspections at Port Elizabeth, Baltimore, and Buffalo: AQIM.
—Proposed MID Inspections Nogales, El Paso, Blaine, and Puerto Rico: AQIM.

Self-Inspection Reporting System (SIRS)

—CBP AIPP also uses the SIRS to monitor the agricultural program and to identify areas for improvement.

—CBP AIPP has developed self-inspection worksheets based on Office of Field Operations (AIPP) policies based on USDA regulations, rules, policies, and needs.
—For example, worksheets target Data Management, Cargo Control, Pest Exclusion, International Mail, and Clearance of Conveyances.

Question. The report claims that the Department has denied APHIS access to port locations when access was requested, even to perform duties for which APHIS still has regulatory responsibility. Is this true and, if so, why was this access denied?

Answer. CBP and USDA–APHIS have forged a new working relationship and resolved many of the earlier port access issues. CBP and USDA employees are working together cooperatively and sharing resources. CBP has worked with USDA to achieve the appropriate level of access to the POEs for their personnel. As Congress has provided, the inspectional functions were transferred from USDA to CBP. CBP has set forth procedures that have facilitated USDA gaining access to the ports to perform their functions.

CBP and USDA–APHIS signed in February 2005 Appendix 8 to Article 8 of the Memorandum of Agreement (MOA) between DHS and the USDA. The MOA establishes and enhances coordinated actions and operations between the two agencies and responds to many of the issues raised in the OIG report.

Question. The report also states that APHIS and the Food Safety and Inspection Service (FSIS) do not require DHS to notify FSIS of all incoming shipments, which could allow the shipments to bypass FSIS re-inspection. Is this correct and, if so, why?

Answer. DHS and USDA are currently developing a MOA to address the data needs of the Food Safety and Inspection Service (FSIS) as well as other USDA agencies.

In conjunction with FSIS, CBP has developed rule sets within our targeting systems to assist with the notification process. CBP and FSIS meet once a week to discuss food safety issues and FSIS has assigned an employee to work at CBP 2 days a week as a liaison. CBP is working very closely with FSIS to make sure that they are properly notified about arriving meat shipments. USDA and FSIS are also working together to update USDA manuals that would require notification of such shipments to FSIS.

Question. Has the Department provided adequate data on staffing levels and deployment of agriculture inspectors to APHIS for evaluation?

Answer. We are unaware of any formal APHIS request for such information nor what type of evaluation is contemplated by the question. However, CBP shares data concerning staffing levels and deployment of CBP agriculture inspection personnel with APHIS regarding training needs for newly hired CBP agriculture specialists in cooperation with CBP and is thus aware of the numbers of new hires.

CBP and APHIS also conduct joint QA port reviews that explore staffing as a standard element. APHIS has identifiers and other personnel at the ports that can verify the staffing levels.

PULSED FAST NEUTRON ANALYSIS

Question. On April 13, 2005, my staff received a report regarding the PFNA program called for by House Report 108–280. This overdue, four paragraph report stated that the contractor testing of this program, which was supposed to have begun in June 2004, been completed by October 2004, with a report issued by December 2004, has "set a firm date of April 18, 2005, for the test to begin." That date has now passed. Did the test start on April 18, 2005? If not, when did or will the test begin? Can you confirm that "the testing will be completed by August 19, 2005, and (that) the test report should reach Congress by November 2005"?

Answer. The operational evaluation of the Pulsed Fast Neutron technology commenced on May 2, 2005, and is scheduled to run for 4 months. An evaluation of the test is expected to be issued in November 2005.

USE OF UNMANNED AERIAL VEHICLES

Question. I understand that the Department has issued a Request for Information to private industry to determine the capability and availability of Unmanned Aerial Vehicle (UAV) systems for use in border control and enforcement. What is the deadline for industry response?

Answer. The RFI for the UAVs was issued on April 13, 2005, and responses were due on April 29, 2005. CBP received 14 responses.

Question. Have you engaged in a dialogue with the private sector about your needs and requirements in this area?

Answer. As noted above, CBP initiated dialogue with the private sector on UAV capabilities and CBP performance requirements through the RFI.

Question. Do you plan to engage in down select and fly-off between competing systems?

Answer. We do not plan to engage in fly-offs between competing systems during down select for the following reasons: the time constraint to establish an Initial Operating Capability (IOC) in fiscal year 2005 does not allow for this, market research resulted in a decision to procure mature commercial off the shelf technology, the development of a refined CBP UAV Performance Specification clearly outlines system requirements, and the RFI included the CBP Performance Specification.

Question. When do you expect a Request for Proposal to come forward and what is the target date to begin acquisition of a system?

Answer. CBP released a Pre-solicitation notice on May 10, 2005, that was followed by an RFP on June 21, 2005, which closed on July 20, 2005. CBP is in the process of evaluating proposals and anticipates a contract award on or about August 29, 2005.

Question. During the period June through September, 2004, there was a pilot program that successfully demonstrated the value of UAVs under the Arizona Border Control Initiative. What were the results of that demonstration and will the lessons learned be incorporated into the Department's long-term acquisition strategy?

Answer. The pilot program demonstrated that the UAVs had some operational effectiveness, but will require further evaluation to determine its optimal deployment. Some of the evaluation criteria were incorporated into the Request for Proposals issued for the purchase of UAVs for CBP. Lessons learned have been incorporated into both the present and long-term DHS acquisition strategies.

Question. I understand that one of the lessons learned from last summer's pilot program was that the initial speed to "get something flying" resulted in some inefficiencies in operation of the system (such as the location of where it was operated and the limited hours it was able to fly) which might have been avoided with proper planning. Are things like this being taken into consideration as you move forward with the program?

Answer. Yes, the lessons learned from the pilot program are being considered as we move forward with the present acquisition. Much attention is being focused on system acquisition, operational procedures and UAV basing to afford DHS the best solution to effectively meet our requirements.

Question. In view of the continuing flood of illegal aliens across the Southwestern Border and the reported success demonstrated with the 2004 UAV program, why hasn't the Department used the $10 million Congress appropriated for UAVs in fiscal year 2005 to restart the demonstration program as an effective enforcement and learning tool while the long term UAV program is developed?

Answer. The Department has evaluated the lessons learned from the two prior UAV deployments and has established UAV requirements that, although mindful of other DHS users, meet CBP's specific needs. A request for proposals was issued in June 2005, and follows the request for information that closed on April 29th. The $10 million in fiscal year 2005 is to be used for a UAV acquisition and subsequent deployment of a UAV system that will serve as the DHS UAV initial operating capability along the Southern border this fiscal year. In the interim, CBP has deployed a Cessna 206 and two Piper Cheyenne airplanes (all equipped with electro optical and infrared sensors) to the Arizona desert to adequately provide aerial surveillance until CBP can acquire and field its own UAVs.

As noted above, DHS is in the midst of a systems-level review of its border control architecture to identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border.

Question. If it chose to do so, how soon could the Department restart that demonstration?

Answer. Since all necessary support requests have since expired, CBP would have to re-negotiate Letters of Procedure with all other airspace managers, a Request for Assistance from the Department of Defense (DOD) to allow us the use of Ft. Huachuca's facilities and logistics, and a Certificate of Authorization issued by the Federal Aviation Administration (FAA) to allow UAVs to operate in the National Airspace System. The earliest the demonstration could be restarted is 60 days from deciding to do so.

DHS "BRANDING" NOT COMPLETED

Question. The Department claims great success with some of its systems integration, including that of its legacy e-mail systems. However, my staff was surprised to learn that one legacy agency—the Federal Protective Service (which transferred over in its entirety from the General Services Administration)—still uses "gsa.gov" for its e-mails as opposed to the DHS "branded" "dhs.gov". What is most troubling

is that the FPS must continue to pay GSA for its e-mail services while also being billed by DHS (or ICE) for these same services—which it is not receiving. Why is there a delay in fully integrating FPS into the Department's operations?

Answer. Fiscal year 2005 resources were committed early in the year to expedite the conversion, which was over 80 percent complete as of March 31, 2005. The remaining Federal Protective Service (FPS) locations were converted by August 19, 2005.

Question. How much has FPS had to pay to GSA for this service this fiscal year to date?

Answer. Fiscal year 2005 GSA charges for FPS information technology support through August 1, 2005, totaled $5,837,498. All FPS offices with the exception of FPS HQ have been converted to the DHS Network. FPS Headquarters is scheduled to relocate from GSA (18th/F) to ICE Headquarters as of August 22, 2005. FPS will reimburse ICE OCIO for services provided.

Question. Since the Department has made claims that all agencies are on the same e-mail system, will the FPS be "made whole" or otherwise reimbursed as a result of these double payments?

Answer. The FPS will fund conversion costs to the DHS email system. FPS has not made, nor will it make, double payments.

C–TPAT

Question. In your statement for the record you say that C–TPAT is due for an increase of $8.2 million and that these funds "will be used to enhance our ability to conduct additional supply chain security validations." Is that the sole purpose for the increase, or will the program also be expanded with these funds?

Answer. CBP intends to use these funds to support the validation process.

Staffing for this program was significantly increased in fiscal year 2005 (120 new positions provided for conducting validations), which will allow CBP to conduct validations of all high-risk supply chains. An aggressive hiring drive to recruit permanent Supply Chain Specialists (SCSs) is underway, and CBP anticipates having 100 permanent SCSs on board at the end of fiscal year 2005. Additionally, CBP has trained 38 field officers to help with the initiation of validations.

As of August 15, 2005, the C–TPAT program has completed validations of 16 percent of certified members, and has validations underway on another 36 percent of certified members.

As of August 15, 2005, the C–TPAT program has over 9,700 applicants, of which 5,174 have been accepted and are certified. With an average of 2,000 to 3,000 new applicants each year, C–TPAT anticipates continued program growth and expansion through fiscal year 2006 and beyond.

Question. Please describe the "security validations" that will be conducted with the proposed increase.

Answer. Validations begin with a domestic corporate meeting. Foreign site visits typically include a corporate meeting with foreign manufacturer corporate personnel, and a tour of appropriate manufacturing, shipping/consolidation and port facilities. Validations conclude with a close out meeting between CBP SCSs and the certified member's Point(s) of Contact(s). The Validation Report issued by the CBP SCS contains sections on Findings, Recommendations and Best Practices.

CBP initiates validations based on risk, using a quantitative risk assessment tool to identify certified members with high-risk supply chains. CBP uses a validation selection methodology that relies upon quantifiable data coupled with an objective assessment of the submitted security profile to determine the top priorities for validations. Validation resources are then directed accordingly.

CBP uses a risk-based approach to validate the security enhancements that have been committed to by C–TPAT members, to evaluate the status and effectiveness of key security measures in the participant's profile, and make recommendations where appropriate. In particular, CBP is placing emphasis on the importer and carrier sectors, and has modified its validation approach to maximize resources and increase efficiencies, such as validating multiple foreign suppliers within a geographic proximity.

Moreover, CBP has enhanced its ability to record and measure validation results by developing the Automated Validation Assessment Tool, which is an electronic questionnaire that automatically scores and weighs the findings of the Supply Chain Specialist to produce an overall assessment of the supply chain security measures in place. Any identified weaknesses must be corrected in order to retain program benefits.

Once the Validation is completed, the C–TPAT partner's role in the process continues as follows:

—Communication on supply chain security issues continues with CBP and the assigned SCS;
—Continual self-assessments of supply chain and security processes and procedures are performed;
—A pro-active approach is maintained with regard to supply chain security and membership in C–TPAT.

ILLEGAL IMMIGRATION

Question. I am concerned that illegal immigrants continue to find new ways into this country. I understand that since the Navy stopped training and steaming in Vieques, Puerto Rico that there has been a surge of illegal immigrants coming to the United States through the Eastern Caribbean into Puerto Rico. What are you doing to close this gap?

Answer. CBP arrest statistics do not substantiate a surge of illegal immigrants through the Eastern Caribbean.

The Office of Border Patrol has one Station and Sector located in Ramey, Puerto Rico. This Sector and Station are located on the Western side of Puerto Rico and respond to their primary threat, which is illegal smuggling through the Mona Passage from the Dominican Republic. Ramey Sector has integrated its Intelligence Unit with other DHS partners to monitor traffic in its area of operation. The Ramey Border Patrol Sector enjoys a cooperative relationship with the U.S. Coast Guard and local Puerto Rican Maritime Police Forces (FURAS). The Coast Guard, Puerto Rican Police, CBP's Air and Marine Office all cooperate on interdictions and landings and share intelligence in a timely manner.

Question. Has there been an increase in the number of illegal alien interdictions or other evidence of an increased flow of illegal aliens to Puerto Rico or Florida from the Eastern Caribbean?

Answer. As noted above, CBP arrest statistics do not indicate that there is an increase in alien apprehensions from countries located in the Eastern Caribbean area or an increase in the flow of illegal aliens from the Eastern Caribbean to Puerto Rico and Florida.

Question. What is the status of discussions to open a Border Patrol Substation in the U.S. Virgin Islands?

Answer. CBP's priority mission is to prevent the entry of terrorists and terrorist weapons into the United States, and agency resources are allocated on the basis of risk assessment. The Northern Border represents a significant terrorist risk due to the presence of terrorist groups within Canada. In addition, aliens from special interest countries have been apprehended crossing the Southern Border using traditional alien smuggling routes. These indicators have to date not been manifested in the Caribbean. Therefore, although CBP continues to work closely with the U.S. Coast Guard to detect and interdict alien and drug smuggling activity in the Caribbean, CBP has not deployed additional resources in the area. CBP's Office of Intelligence is currently conducting a comprehensive risk analysis of the Caribbean, which will form the basis for making a future decision regarding the location of Border Patrol stations in the region.

COLLECTION OF ANTIDUMPING AND COUNTERVAILING DUTIES

Question. Senate Report 108–280 included specific language that directed Customs and Border Protection (CBP) to submit a report to the House and Senate Appropriations Committees by February 8, 2005. The report was to provide a coordinated plan, including legislative or regulatory changes proposed by CBP, if necessary, to increase CBP's collection of antidumping and countervailing duties owed to the United States. The Senate Appropriations Committee has not yet received that report. Will the report be delivered prior to the Subcommittee marking up the fiscal year 2006 bill in June?

Answer. The report was sent to the Committee on July 7, 2005.

Question. On December 17, 2004, Customs and Border Protection issued its regular Annual Report on the Combined Dumping and Subsidy Offset Act (CDSOA). The Annual Report described how hundreds of millions of dollars in duties are not being collected by Customs, and the agency has been unable to explain why it cannot collect these funds. In fiscal year 2003, the agency failed to collect $130 million in duties owed the United States under the U.S. antidumping and countervailing duty laws, and CBP failed to collect an additional $260 million in fiscal year 2004. The majority of that $390 million is the result of uncollected duties on goods imported from China.

What is CBP doing to solve this problem?

Answer. CBP disburse annually all antidumping duties available from entries that have been finally liquidated to domestic petitioners. The disbursements are made within 60 days of the end of the fiscal year.

CBP recognizes that imports of antidumping merchandise pose a financial risk to domestic industry. We share the concern regarding the lack of funds available for disbursement to domestic petitioners of antidumping duties. Therefore, CBP has instituted several aggressive actions to mitigate the collection risks going forward. We have a high degree of confidence that for entries received after the initiation of these new measures, the collection rate will improve.

—*Amendment to the Continuous Bond Guidelines.*—As of July 9, 2004, CBP has increased the continuous bond amount for importers of agriculture/aquaculture products subject to antidumping cases. The bonds will be set at a much higher rate, providing additional coverage in the event that an importer defaults. The new and proactive approach by CBP will provide the highest level of protection against default and directly addresses instances where the final liquidation rate is much higher than the initial deposit rate made at time of entry.

—*Integration With Other Agencies.*—CBP has recently begun working with the Department of Treasury to address the financial risks associated with sureties. Treasury conducts quarterly solvency evaluations of sureties and provides approval of the sureties to write customs bonds. By working together, we have developed a mechanism by which CBP can provide Treasury with data about sureties that are heavily weighted in "high-risk" transactions, such as antidumping. Treasury will incorporate this information in their solvency evaluation to mitigate the risk of surety bankruptcy. In addition, CBP is closely working with the Department of Commerce to find workable solutions to the challenges we face in collecting antidumping duty.

—*Increased Monitoring of Imports.*—CBP has taken measures to increase the monitoring of entries of agriculture/aquaculture products subject to antidumping duties. This monitoring provides a means to ensure compliance with bonding requirements, aids in the identity of surety risks, and helps thwart circumvention attempts. The closer scrutiny allows CBP to quickly identify new importers, particularly sham or shell companies. The monitoring provides CBP with the opportunity to raise bonds on these entities at once. By stepping up the monitoring of agriculture/aquaculture imports, CBP is also in a position to recognize shifts in patterns that may indicate circumvention attempts.

We believe that the new bonding methodology, working with other agencies, and closely monitoring imports will have a positive impact on the collections of antidumping duty, making more funds available for disbursement to the domestic industry.

CBP has taken a number of steps to ensure that the appropriate antidumping and/or countervailing duty (AD/CVD) revenue is collected. CBP has initiated centralization of all AD/CVD continuous bond activity for the bond program under the Revenue Division, Office of Finance, U.S. Customs and Border Protection in Indianapolis, Indiana. This establishes more uniform, consistent and effective management of continuous bonds involving AD/CVD. Also, AD/CVD bond formulas have been amended with an objective to minimize AD/CVD revenue losses as a result of bond insufficiency. The first commodity subject to this new bonding formula is shrimp.

Question. Why is this problem of non-collection growing, and what is CBP doing to address it?

Answer. Final liquidation for AD/CVD occurs several months, sometimes years after actual entry of the merchandise. The significant increase in uncollected antidumping duties seen in fiscal year 2003 reflected the first series of liquidation instructions for cases covering the types of merchandise we now understand to be problematic for collection; agriculture/aquaculture merchandise. These liquidation instructions covered entries going back as far as 1997 and 1998. The increase in uncollected antidumping duties in fiscal year 2004 reflects the growth in imports that was seen in years after the initiation of the cases, particularly the crawfish case. CBP is confident that collection rates will increase for entries received after the implementation of the measures highlighted in above.

CBP has taken several measures to maximize collection of AD/CVD revenue. Continuous bonds covering new AD/CVD merchandise are being managed as a part of the overall centralization of continuous bonds at the Revenue Division, Office of Finance, U.S. Customs and Border Protection in Indianapolis, Indiana. Also, AD/CVD bond formulas have been amended with an objective to minimize AD/CVD revenue losses from bond insufficiency. However, uncollected revenue will occur as a result of entry activity during years prior to affecting these new measures. As an example, although the Revenue Division has processed over 25,000 continuous bonds from the beginning of the centralization effort that began August 12, 2003, not one bond has

been subject to a collection action. Collection action is dependent on liquidation of the formal entry summaries covered by the bond. Liquidations may occur up to several years following the initial entry date. In addition, the amended AD/CVD bonding formula currently covers only shrimp.

Question. In past correspondence with my office, Commissioner Bonner indicated that CBP supported legislation that Senator Cochran and I introduced in the last Congress—and that we have reintroduced in the 109th Congress—to solve this problem of non-collection. That legislation, which passed the Senate unanimously last year, would require cash deposits instead of bonds in certain antidumping reviews. Would you be willing to express your support for this legislation directly to House Ways & Means Chairman Bill Thomas and other Members of the Congress, including the House leadership?

Answer. The Department and CBP are taking steps necessary to collect appropriate duties and provide appropriate funds to U.S. companies and workers through the Continued Dumping Subsidy Offset Act (CDSOA) disbursements. We agree that cash deposits in lieu of single-entry bonds may provide greater coverage and are less of an administrative burden. We are taking steps to provide greater security for the collection of AD/CVD within the framework of existing legislation, and are working with the Department of Commerce to apply more innovated methods to address these and other risks from imports subject to antidumping and countervailing orders. We look forward to continuing to work with Congress on ways to improve our performance in this area.

Question. As mentioned previously, in the past, U.S. industries like the U.S. crawfish industry have discovered only very late in the year that millions of dollars of antidumping duties for some reason have not been collected in their cases against Chinese imports as required by law. And, because CBP's failure to collect these duties has been discovered late in the year, the non-collection problem in these cases could not be addressed in time to enable the industries to obtain their yearly distribution of funds under the CDSOA. As a consequence, the U.S. crawfish industry, for example, last year failed to receive at least $54.4 million it otherwise would have received in duties paid the U.S. Government by Chinese importers. It is my understanding that CBP's Office of Information Technology (OIT) is fully capable of running an already existing program much earlier in each calendar year, (meaning by the end of March at the latest), which would enable both CBP and U.S. industries to learn, much earlier, if millions of dollars in duties are not being collected by CBP from U.S. importers of foreign, dumped products.

Why can't CBP's OIT determine by the end of this month if there are cases in which CBP is not collecting duties owed the U.S. Government and make that information publicly available as early as possible?

Answer. CBP has responded to the revenue risk posed by the inability to collect certain AD/CVD duties through several means, one of which is the monitoring the AD/CVD bills and collections on a more regular basis. For the distribution of these funds to take place timely, it is necessary not only to monitor the timely collection of AD/CVD duties but also to ensure our revenue collection system is protected from possible circumvention and corporate solvency schemes designed to enter AD/CVD goods into the U.S. market with the intention of never paying the proper duties at time of liquidation.

On a monthly basis, CBP is performing a risk-based review of outstanding bills for AD/CVD duties. The information has proven effective in identifying high-risk companies for AD/CVD evasion as well as improves the timeliness of our reviews. CBP is also focused on the long-term issue of the company's financial solvency and their ability to pay outstanding AD/CVD bills. The continuous bond guidelines for imports of certain agriculture/aquaculture imports were amended in July 2004 to address just such an issue. Working with the Department of Commerce, we are addressing the AD/CVD issues that pose the greatest risk.

Question. Again, two of the problems that CBP has exhibited with respect to its administration of the CDSOA are (1) CBP failure to collect duties rightfully owed; and (2) its failure to pay duties already collected in a timely fashion to eligible U.S. companies and their workers. With respect to the second problem, CBP sometimes holds, in what are called "clearing accounts," duties that are collected over many years—but for which the agency is awaiting final "liquidation instructions" from the Commerce Department prior to distribution. Often, the Commerce Department claims that such instructions have been sent, but CBP does not know they have been sent or never receives them. It has been proposed that one solution to this problem would be for CBP to publish the amount of funds held in CBP's clearing accounts, by administrative review period, so that CBP and Commerce can work together to determine which funds should have been liquidated and be available for distribution to eligible U.S. producers. CBP, in certain circumstances, has provided

such information to Members of Congress upon request, but has refused to provide such information generally.

Will you commit to identifying (i.e., publishing) the amount of funds held in clearing accounts by administrative review period?

Answer. The AD/CVD modules within the Automated Commercial System (ACS) do not provide information by administrative review periods; therefore, CBP cannot currently track entries in this manner. CBP has provided information of this type in certain circumstances through a manual review process. CBP is working towards including functionality in the Automated Commercial Environment (ACE) to identify and track AD/CVD data to ensure timely and accurate liquidation.

The OIG expressed concern about approximately one million entries suspended by CBP. As a result of this finding, CBP developed a plan to isolate those suspended entries that were beyond the normal timeframes of an AD/CVD case. Once identified, CBP worked with the Department of Commerce (DOC) to obtain liquidation instructions for these entries. To date, CBP has reduced the national inventory by 80,000 entries. CBP plans to continue to work with DOC to reduce the inventory substantially.

In fiscal year 2005, CBP is concentrating on the liquidation of remaining AD/CVD entries entered prior to 1995 that remain suspended. This action will remove approximately 50,000 entries representing over $46 million in deposits on 222 cases from the "official" inventory. By the middle of fiscal year 2006, CBP plans to liquidate the remaining 50,000 or so entries.

Another reason that monies remain in the "clearing accounts" and are unavailable for distribution via CDSOA is the number of protests on bills issued by CBP. Payment of a protested bill is deferred until the protest decision is rendered. Currently, many protests of AD/CVD liquidations are suspended pending the final decision by the Federal Appeal Court on International Trading.

Question. Will you commit similarly to identifying the reasons for the lack of liquidation in cases where liquidation has not occurred for more than 4 years, and provide specific information with respect to those cases showing the amounts that remain unliquidated accompanied by an explanation of CBP's understanding of why the amounts have not been liquidated?

Answer. Again, the AD/CVD modules within the ACS do not provide information by administrative review periods; therefore, CBP cannot track entries this way. This functionality will be programmed into the ACE and should be available by the end of fiscal year 2007.

STAFFING

Question. What was the CBP on-board strength (including AMO) on September 30, 2004? What was it on March 31, 2005? Provide the same data for the Border Patrol.

Answer. Air and Marine Operations employees were not transferred to CBP until October 31, 2004. The attached chart therefore provides on-board strength at two snapshots in time to reflect this transfer.

	October 2, 2004	April 2, 2005
Total CBP staffing		
CBP total	40,934	41,717
Border patrol agent staffing		
Border patrol Agents total [1]	10,817	10,859

[1] These amount are also included in the CBP totals above.

DETENTION FACILITIES

Question. One of the primary functions of the Bureau of Immigration and Customs Enforcement (ICE) is to serve as this country's interior line of defense by apprehending illegal entrants and detaining them pending the outcome of an administrative determination of their status. However I understand that ICE is considering closing the only secure, non-criminal detention center in New York City—the very site of the 2001 terrorist attacks—because of an apparent decision to focus the bulk of the agencies efforts on only identified criminal aliens and other high-risk illegal immigrants. This concerns me greatly because I understand that the vast majority of the individuals detained at this New York City detention facility would be released on their own recognizance into the New York City area.

Why is DHS proposing to close this detention facility in New York City? Is this because of a lack of funds? Are there not enough aliens needing to be detained which necessitates the closure of this facility?

Answer. In a continuing effort to consolidate detention capacity where possible in order to increase operational efficiency, ICE has decided not to exercise the next available option to extend contract performance at the Queens CDF.

The current contract was awarded to GEO on March 27, 2002. The Queens CDF provides detention housing and transportation of non-criminal detainees in the custody of ICE. A significant population designated to the Queens CDF is comprised of asylum seekers apprehended at POEs in the New York area.

The indefinite delivery/indefinite quantity contract includes a guaranteed minimum detainee population of 150 ($219.02 per manday) and a maximum capacity of 200 ($9.17 per manday exceeding 150 beds). The contract consists of a base year and 4-1 year options, exercised at the unilateral discretion of the government. The contract is currently performing within Option Year 2.

A recent assessment determined that a substantial number of the population routinely designated to the Queens CDF could be adequately managed through a combination of bonds, orders of own recognizance, and/or the increased use of alternatives to detention (e.g., electronic monitoring; telephonic reporting, etc.). All non-detention options will be applied based on established ICE standards. The remaining population requiring detention can be consolidated into substantially lower cost detention capacity available to ICE via commercial contracts and agreements with local government service providers. Other efficiencies will accrue from the consolidation of detainees, staff, the administrative hearing process, support programs, etc. These increased efficiencies will permit ICE to apply funds toward detaining higher priority cases.

It should also be noted that various non-governmental organizations have previously expressed concern regarding conditions of confinement at the Queens facility (See February 8, 2005 CIRF report, "Report on Asylum Seekers in Expedited Removal).

Utilizing all available options to manage the non-criminal alien population apprehended in the New York area and consolidating the population requiring detention into lower cost facilities, will result in improved efficiency in the ICE detention program.

Question. I understand that ICE makes an initial determination as to the level of risk of the illegal alien and that such a determination often is conducted at the point of entry which, in the case of this facility, is JFK International Airport.

How often does ICE make an initial determination that an individual is a "low-risk" illegal immigrant and then, after further investigation, determine that the individual should have been classified as "high-risk?"

Answer. The law enforcement databases used to track alien detention do not allow for us to determine the number of aliens who were initially considered "low risk" and are then later considered "high risk". These categories are used as guidelines in making the detention decision, but are not recorded as such in these databases.

Question. I believe these non-criminal detention facilities serve several purposes, one of the most important of which is holding those potentially high-risk individuals who fall through the cracks during the initial screening and who initially are misclassified as low-risk. Furthermore, I believe that facilities such as the one in New York City serve a very important deterrent effect. I understand that JFK Airport was a popular entry point for illegal immigrants prior to the opening of this New York City detention facility.

Does DHS believe that these types of facilities serve a deterrent effect and, more importantly, serve to catch high-risk individuals who might slip through the initial screening process?

Answer. Detention and removal are deterrents to illegal immigration. However, detention resources must be effectively managed to ensure that secure capacity is available to accommodate cases according to our detention priority continuum. It has been determined that a substantial number of the population routinely designated to the Queens CDF could be adequately managed through a combination of bonds, orders of own recognizance, and/or the increased use of alternatives to detention (e.g., electronic monitoring; telephonic reporting, etc.). All non-detention options will be applied based on established ICE standards. The remaining population requiring detention will be consolidated into substantially lower cost detention capacity available to ICE via commercial contracts and agreements with local government service providers. Other efficiencies will accrue from the consolidation of detainees, staff, the administrative hearing process, and support programs. These increased efficiencies will result in savings that can be applied to other immigration enforcement activities.

Question. Given the importance of these types of facilities, how can DHS justify their closure in New York City, especially when the only other facility in the general vicinity is designed to hold criminal aliens and which I understand operates at or near capacity?

Answer. A recent assessment determined that a substantial number of the population routinely designated to the Queens CDF can be adequately managed through a combination of bonds, orders of own recognizance, and/or the increased use of alternatives to detention (e.g., electronic monitoring; telephonic reporting, etc.). All non-detention options will be applied based on established ICE national standards. The remaining population requiring detention can be consolidated into substantially lower cost detention capacity available to ICE via commercial contracts and agreements with local government service providers. All cases requiring detention will be designated to appropriate conditions of confinement. Efficiencies will accrue from the consolidation of detainees, staff, the administrative hearing process, and support programs. ICE can use the savings from these increased efficiencies to detain higher priority cases.

MEASURES FOR DETERMINING BUDGETS

Question. What is the ratio or other measurement by which ICE determines how many detention beds are required in a given year? For instance, is there a ratio or determination made such that if one assumes that one Border Patrol agent is responsible for *x* apprehensions of illegal aliens then there is a need for *y* detention beds? And is there a similar ratio or measurement between the amount of bed space required because of the investigation success rate of ICE immigration investigators?

Answer. The Department is working aggressively to develop a comprehensive border control strategy that responds more effectively to alien apprehensions and the overall flow of illegal crossings. As fundamental improvements to the system are implemented through this strategy, we will implement systematic modeling that can more accurately link resources with apprehensions and other measures of demand.

WORKSITE ENFORCEMENT

Question. For Worksite Enforcement, how does ICE determine how it will focus its resources? For example, which areas or industries will be targeted?

Answer. Since September 11, 2001, ICE Worksite Enforcement activities have focused primarily on removing unauthorized workers from critical infrastructure facilities to reduce the risk of terrorist attack from insiders. ICE Critical Infrastructure Protection (CIP) operations are generally initiated at the local level and are based upon factors such as the type and number of infrastructure facilities present in each Special Agent-in-Charge jurisdiction (seaports, airports, military bases, defense contractors, nuclear plants, etc.) and upon specific or general threat information received from various intelligence sources, the general public, and from other law enforcement agencies.

ICE Worksite Enforcement activities also target criminal employers whose violations have a nexus to human smuggling, immigration document or benefit fraud, and worker exploitation. The authorities being enforced generally include one or more of the civil and/or criminal provisions of INA 274A (Unlawful Employment of Aliens). Many criminal employer investigations also result in the charging of violations relating to harboring, smuggling, and document fraud. The fiscal year 2006 Budget includes an increase of $18 million and an additional 140 agents to support the Temporary Worker Program.

CYBER CRIMES

Question. For fiscal year 2005, Congress provided $4.2 million for additional cyber crime forensic infrastructure and expansion of the Cyber Crime Center to ICE field offices. What is the status of this effort?

Answer. This funding provides for the creation of a wide area storage network for the ICE Computer Forensic Program. Upon award, disk storage arrays will be installed in four or five (final numbers are contingent upon final pricing) ICE field offices to provide storage for digital evidence under examination.

The ICE Cyber Crime Center has conducted a thorough market and technical analysis and is in the final stages of making a vendor selection.

An inter-agency agreement has been established with the U.S. Bureau of Public Debt (BPD) to utilize their existing IT procurement vehicle to make the contract award. The statement of work and performance work standard documents have been forwarded to BPD on August 18, 2005. It is anticipated that the contract will be awarded to TKC Communications of Fairfax, VA, an Alaskan native corporation,

shortly. Once awarded, site surveys, selection, and installations will begin in earnest.

Question. Have any of these funds been obligated?

Answer. None of the $4.2 million has been obligated.

Question. Have any additional personnel been hired?

Answer. No additional personnel will be hired with the $4.2 million.

Question. To which field offices, if any, will the Center expand?

Answer. This answer contains infomrmation considered Law Enforcement Sensitive and has been provided to the Committee under separate cover.

PASSENGER AIR FEES

Question. The Administration's budget for DHS proposes a significant increase to the security fee passengers pay by more than doubling the cost for the first leg of a flight from $2.50 to $5.50. These fee collections, if approved, would be used to pay for approximately 83 percent of the fiscal year 2006 budget request for the Transportation Security Administration. According to the Congressional Budget Office (CBO), this proposal would generate $1.680 billion in additional funding for fiscal year 2006.

Will a legislative proposal be sent to the authorizing committees with jurisdiction over this issue, and if so, when?

Answer. The fiscal year 2006 President's Budget provided a legislative proposal to modify this fee authority. In Title V—General Provisions, the proposal states, "SEC. 517. In Chapter 449 of title 49, United States Code, section 44940(c) is amended by striking '$2.50' and replacing it with '$5.50', and striking '$5.00' and replacing it with '$8.00'." This modification to the fee authority would allow TSA to implement the fee increases sought in the President's fiscal year 2006 Budget. TSA will work with the Appropriations Committees of the House and the Senate, as well as the appropriate authorizing committees in both bodies, to ensure enactment of the proposed security service fee increase.

Question. Second, if the proposed fee is not approved, will the Secretary urge the President to submit a budget amendment to fill the $1.7 billion funding gap?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

Question. Finally, what programs and activities does the Department propose be cut if the fee increase is not authorized by Congress?

Answer. The sharing of aviation screening costs between industry, passengers, and Government is essential to ensure that there is sufficient funding for existing and emerging threats to the integrity of the aviation security infrastructure. The proposed increase is intended to shift the burden of paying aviation screening services from the general taxpayer to the airline passenger. The Department will work with Congress to ensure that security priorities are met.

AIR CARGO

Question. Public Law 108–458, which was signed into law by the President on December 17, 2004, included an authorization for $100 million in fiscal year 2006 to accelerate the development of technologies to screen air cargo. The Administration's budget proposes that air cargo screening technology development be funded through the Science and Technology directorate, but funding is cut by $45 million from last year and funding is $70 million below the amount authorized in the Intelligence Reform Act. How is a cut of this magnitude justified? Has there been a break through in the development of detection technology for air cargo that justifies the proposed cut?

Answer. The fiscal year 2006 President's Budget transfers $109 million in R&D funds from TSA to the S&T Directorate. Of this amount, $29.578 million is dedicated to projects that will address air cargo screening capabilities. TSA retains $23 million in its fiscal year 2006 request to continue analyzing EDS products emerging from the Phoenix Phase II R&D program, piloting passenger screening projects, including next generation trace portal and automated checkpoint EDS, continuing EDS cargo break bulk evaluation, and conducting cargo technology field evaluations for field experiments.

The S&T Directorate does not plan to fund consolidated air cargo technology development outside those efforts captured by our broad R&D program, or captured in other efforts within the directorate, such as RFID technology, unless air cargo

pilots demonstrate the need and utility in specific cases, and focus instead on break-bulk inspection. Given a break-bulk inspection paradigm, the same technologies being explored for package or luggage inspection apply to cargo screening—and thus it is straightforward to include consideration of any specific requirements, e.g., size and throughput, into our broad R&D program.

With the fiscal year 2006 R&D funds, the S&T Directorate plans to conduct broad R&D that is applicable across the spectrum of baggage, package, and cargo screening. The S&T Directorate estimates that the funding required in fiscal year 2006 to complete the assessment of the efficacy of specific existing methodologies for particular cargo commodities, and to test screening procedures in the laboratory would be approximately $5 million. The Phoenix project is aimed at reducing false alarm probabilities in EDS systems, which is clearly beneficial to both baggage and package inspection. Other relevant RDT&E efforts within the aviation explosives detection efforts include nanotechnology-based sensors, CT array-based imaging (as opposed to rotating scans), and improved trace systems. Some of the TSA R&D projects funded in fiscal year 2005 will continue into fiscal year 2006 through completion of prototypes. These projects may continue to be funded by the S&T Directorate if they meet certain criteria, particularly in the area of break-bulk inspections.

Question. Public Law 108–458 authorizes $200 million per year for TSA to improve aviation security related to the transportation of cargo on both passenger aircraft and all-cargo aircraft. Why doesn't the fiscal year 2006 request include additional funding for air cargo security?

Answer. TSA's request for air cargo resources is at an appropriate level to ensure air cargo security and recognizes non-recurring system development costs while at the same time meeting all of the necessary transportation security priorities.

Question. Are there plans to increase the number of inspectors?

Answer. TSA currently employs 196 cargo inspectors. Three others have been selected and are in the final stages of the hiring process.

Question. Is TSA satisfied with 200 air cargo inspectors?

Answer. The President's fiscal year 2006 Budget request is a reflection of the resources required to ensure air cargo security and recognizes non-recurring system development costs while at the same time meeting all of the necessary transportation security priorities. Going forward, TSA will evaluate the needs and resources available to determine whether additional inspectors would be appropriate.

PRE-PACKAGED NEWS

Question. On March 16, the Washington Post printed an editorial entitled Viewer Beware. The editorial questioned the use of government-packaged and government funded news reports to look and sound like regular television reports. The editorial stated "Although this Administration apparently isn't the first to use video news releases, it seems more enamored of them than its predecessors. For example: A spot commissioned by the Transportation Security Administration lauds "another success" in the Bush Administration's drive to strengthen aviation security," which the reporter describes as "one of the most remarkable campaigns in aviation history." Unbeknownst to the viewer, the so called reporter was no reporter at all. She was a contractor hired by TSA. This type of pre-packaged reporting has occurred in other agencies as well, such as the Office of National Drug Control Policy (ONDCP) and the Department of Health and Human Services.

In every year since 1951, Congress has included a provision in the general government appropriations act which states the following: "No part of any appropriation contained in this or any other Act shall be used for publicity or propaganda purposes within the United States not heretofore authorized by Congress."

In recent cases involving prepackaged news stories by ONDCP and the Department of Health and Human Services, GAO concluded that those prepackaged news stories violated the publicity or propaganda prohibition. GAO did not receive a request to review the TSA story, but it was developed in a similar manner.

The Senate recently approved by a vote of 98–0 an amendment to the emergency supplemental to prohibit Federal funding of pre-packaged news stories unless the story includes a notification that it was created and funded by a Federal agency.

Do you agree that pre-packaged news segments produced by any DHS office should include a clear notification to the audience that the story was prepared or funded by that Federal agency?

Answer. DHS has a unique responsibility to provide Americans with important information they can use to be prepared for disasters, terrorist attacks or even to better navigate security procedures at our airports and ports-of-entry. Video news releases can serve as one tool for accomplishing this objective. We agree with the Ad-

ministration's previously articulated position that Federal agencies should be open about their activities and that DHS-produced Video News Releases (VNRs) should be clearly marked.

SCREENING WORKFORCE PERFORMANCE

Question. The DHS Inspector General recently released results of an audit on Transportation Security Administration screener performance.

The IG's audit indicated that the problems will most likely persist without greater use of new technology. The IG recommended that the TSA administrator aggressively pursue the development and deployment of innovations and improvements such as the backscatter x-ray and explosive trace detection portals to help the screener workforce better detect weapons and explosives. However, the Department's fiscal year 2006 budget actually reduces the amount of money included for Next-Generation explosive detection systems from $54 million to $49 million and significantly below the $100 million authorized in the Intelligence Reform Act.

In light if the sobering results of the IG audit, how can you justify reducing the amount of funding for the development and deployment of innovative detection technologies?

Answer. The TSA recognizes that additional resources must be devoted to address this critical vulnerability and improve the effectiveness of checkpoint screening. As it relates to deployment, TSA will have the ability to screen elevated risk passengers for explosives at all passenger checkpoints by January 2006. TSA will devote a total of $100 million to this initiative in fiscal years 2005 and 2006. In fiscal year 2005 TSA received $28.3 million to field emerging technology equipment at checkpoints. For fiscal year 2006, TSA is requesting a total of $72 million (an increase of $43.7 million over the fiscal year 2005 base amount) for emerging checkpoint explosives technology. In fiscal year 2005, TSA devoted $54 million for research and development (R&D) on Next Generation Explosives Detection Systems (EDS). The fiscal year 2006 Budget proposes to transfer TSA's R&D function to the S&T Directorate.

TSA SPENDING ABUSES

Question. The DHS Inspector General recently released a report that highlighted a laundry list of disturbing financial purchases relating to the creation of the Transportation Security Operations Center. For instance, $252,000 was spent on artwork, $30,000 was spent on expensive silk plants, money was used to buy leather brief cases and coffee pots, and over $83,000 in overpayments remains unaccounted for. There are even seven kitchens in the building for just 79 Federal employees located there. This report follows on the heels of the IG's findings last year that TSA provided excessive bonuses to its executives.

In response to these findings, A TSA spokesman said that "a new management structure" has been put in place "to strengthen its acquisition program to ensure responsible stewardship of taxpayer dollars." Please explain in detail what steps have been taken to change TSA's management structure to prevent such abuses from continuing.

Answer. Since its inception, TSA has worked to develop and implement a more responsive and robust acquisition program based on sound business management practices. The elevation of the Office of Acquisition within the agency is a key indicator of our commitment. Since the Transportation Security Operations Center (TSOC) lease process was initiated, the Office of Acquisition has been elevated to the Assistant Administrator level, equivalent to the Chief Financial Officer (CFO) rather than as a sub-program within the CFO's office. In late 2003, the Office of Acquisition stood up an Acquisition and Program Management Support division to focus on certifying, training, and providing day-to-day assistance to and for TSA's program managers. Well over 1,200 TSA employees have been trained to date in key acquisition topics and the Program Management certification program is robust.

At the beginning of fiscal year 2005, TSA took the following steps to help strengthen and mature its acquisition program in four key areas.

—Continue to support the TSA mission with efficient, expeditious, and accurate contracts. TSA recognizes that the agency's ability to attract, recruit, and retain qualified acquisition personnel to support contracts is critical to fulfilling its mission. Initial staffing in the Office of Acquisition was barely adequate to award contracts in time to meet Congressional deadlines, much less commence good business processes. Over the past year, TSA has raised the Office of Acquisition's staff ceiling by nearly 30 percent. Additionally, a percentage of TSA's budget has been earmarked for contract oversight, which includes support from

the Defense Contract Audit Agency and Defense Contract Management Command, and independent contractor support.

—Significantly improve acquisition and program planning. The Office of Acquisition is focused on strengthening the program planning function. The office developed and now coordinates an Investment Review Board process that drives successful program decisions by providing direct subject matter expert support to program managers. Additionally, the office provides direct support to program offices to assist them in developing sound acquisition and program strategies.

—Significantly improve program management and administration. Well-trained, certified program managers are fundamental to robust acquisition programs. These managers were, initially, in short supply at TSA. To address immediate knowledge gaps in key areas, the Office of Acquisition rolled out a set of workshops in October 2003. In early 2004, TSA worked with DHS to implement a Program Management certification program and the first TSA applications were received in June of 2004. Moreover, the Office of Acquisition developed a Management Directive regarding acquisition planning, review, and reporting that significantly tightens up the overall process.

—Build and mature the TSA acquisition infrastructure. TSA is focused on these two infrastructure areas: human resources and systems.

Human Resources.—In addition to increased staff, the Office of Acquisition is developing a longer-term strategic human capital plan to manage recruitment and retention issues, provide for career development, and succession planning. The plan will provide a roadmap for strengthening the current workforce (training, communication, professional development), as well as outline strategies to recruit highly qualified individuals and manage attrition. Simply put, the strategy will outline a plan to develop the right people with the right knowledge and skills for each of TSA's acquisition programs.

Systems.—On the systems level, TSA is implementing PRISM, an integrated finance and procurement system which will streamline and strengthen our processes and integrate acquisition with finance and asset management.

AIR CARRIER FEES

Question. The Government Accountability Office recently estimated that 2000 passenger and property screening costs incurred by air carriers was $448 million, $129 million less than what the air carriers paid to TSA. What plan of action will be taken by TSA as a result of GAO's estimates?

Answer. In the Homeland Security Appropriations Act, 2005, (Public Law 108–334) Congress directed the Government Accountability Office (GAO) to determine how much air carriers spent on security screening in 2000—the basis for the fee imposed on airlines. GAO completed its review and issued a report on April 18, 2005. The report concludes that the amount of the industry-wide passenger and property screening costs was between $425 million and $471 million, with a midpoint estimate of $448 million. The midpoint difference between what is collected now and what GAO indicates should be collected is $129 million. However, GAO's estimate did not include certain cost categories (e.g.; real estate, CAPPS, and positive bag match) due to the unavailability of information within the timeframe provided. The cost of these items could be significant. The TSA is currently reviewing all the findings of the report and developing a suitable overall implementation strategy for the air carrier fee.

SECTION 605 OF VISION 100

Question. The TSA budget proposes to defer use of allocation formulas required by Section 605 of Vision 100. Please provide a list, by airport, of all requests for assistance under the allocation formula program versus funding provided via Section 605. This list should distinguish between large hub airports, medium hub airports, and small hub airports.

Answer. TSA has received a number of requests from airports for funding to support construction of, or reimbursement for, in-line checked baggage screening solutions. Below is a list of the airports that have made these requests:

	Airports that have requested funding for an Inline System	Category	Notes
BWI	Baltimore-Washington International Airport	L	
DCA	Ronald Reagan Washington National Airport	L	
DTW	Detroit International Airport	L	
EWR	Newark International Airport	L	

	Airports that have requested funding for an Inline System	Category	Notes
FLL	Ft. Lauderdale-Hollywood International Airport	L	
HNL	Honolulu International Airport	L	
IAD	Washington-Dulles International Airport	L	
IAH	George Bush Houston Intercontinental Airport	L	
JFK	John F. Kennedy International Airport	L	
LGA	LaGuardia Airport	L	
MCO	Orlando International Airport	L	
MDW	Chicago Midway International Airport	L	
MIA	Miami International Airport	L	
MSP	Minneapolis-St. Paul International Airport	L	
OAK	Metropolitan Oakland International Airport	L	
ORD	Chicago O'Hare International Airport	L	
PHL	Philadelphia International Airport	L	
SAN	San Diego International Airport	L	
SFO	San Francisco International Airport (reimbursement)	L	
SLC	Salt Lake City International Airport	L	
TPA	Tampa International Airport	L	Current in-line system
ANC	Anchorage International Airport	M	
BDL	Bradley International Airport	M	
BNA	Nashville International Airport	M	
CLE	Cleveland-Hopkins International Airport	M	
MCI	Kansas City International Airport	M	
MKE	General Mitchell Milwaukee International Airport	M	
OGG	Kahului Airport Maui	M	
PDX	Portland International Airport	M	
PVD	Providence T F Green State Airport	M	
RSW	Southwest Florida Fort Myers International Airport	M	
SAT	San Antonio International Airport	M	
SJC	San Jose International Airport	M	
SMF	Sacramento International Airport	M	
SNA	Orange County John Wayne Airport	M	Current in-line system
BIS	Bismark Municipal Airport	N	
LNK	Lincoln Municipal Airport	N	
ACY	Atlantic City International Airport	S	
GEG	Spokane International Airport	S	
GPT	Gulfport-Biloxi International Airport	S	
MDT	Harrisburg International Airport	S	Current in-line system
PSP	Palm Springs International Airport	S	
TLH	Tallahassee Regional Airport	S	
VPS	Okaloosa Regional Airport	S	

Category: small (s), medium (m), large (l) or non-hub (n).

BASE DECREASES

Question. On page 38 of the TSA budget request, there is a reduction of $15.9 million for "management and technology efficiencies" and a reduction of $53.9 million for a "base realignment adjustment." There is no additional justification or information relating to those reductions. Provide a detailed justification for those decreases including a list of all management and technology efficiencies and how realigning the base saves $53.9 million.

Answer. The attached spreadsheet provides a detailed explanation of program reductions and base adjustments that resulted in $53.9 million in savings.

	FY2006 Proposed Spendplan	FY 2005 Enacted	Annualization of FY 05 Pay	Efficiency[1]	PAY/ NON PAY	Xfer Out	Remix & Program Decreases	Total FY 06 Base	Passback/Final Appeals Apprvd	Total	Comments
I. Aviation Security											
A. Screening Operations											
1 Screener Workforce	**2,557,001**	**2,424,000**						**2,489,003**		**2,668,984**	
Privatized Screening	152,854	129,654		(436)	1,985			131,151	15,000	146,151	Funding to support continued PP5 operations & increase workman comp. Bill.
Screener-PC&B	2,404,347	2,294,346	11,174	(8,943)	61,275			2,357,852	164,981	2,522,833	Funding required to support 45K screener FTE reflects a base adjustment.
2 Screener Training and Other	**438,574**	**494,274**						**468,484**		**468,484**	
Screener Consumable Supplies & Other	122,217	187,071		(751)	3,051		(31,328)	158,043		158,043	In order to stay within FY06 budgetary constraints, TSA scaled back field operations travel/consumables, uniforms, tort claims and preventative maintenance purchases to provide an offset for screener pay and benefits, human resources (HR) services, and in
Screener Training	94,354	145,000		(544)	2,220		(55,872)	91,004		91,004	Increasing the number of training classes conducted by TSA Approved Instructors and decreasing contractor instructed training.
Representation Funds	3	3						3		3	
HR Services	210,200	150,000		(563)	2,297		55,500	207,234		207,234	Funding required to support 45K screener FTE reflects a base adjustment.
Model Workplace	2,200	2,200					200	2,400		2,400	
Hazardous Material Disposal	9,600	10,000					(200)	9,800		9,800	
3 Checkpoint Support	**125,109**	**123,500**						**113,761**		**157,461**	
Checkpoint Reconfiguration	13,200	13,200		(75)	245		(3,370)	10,000		10,000	
Magnetometers	1,809										In order to stay within FY06 budgetary constraints, TSA reduced the rate of purchasing new checkpoint equipment, emerging technology, and electronic surveillance equipment for airports to ensure adequate funding for existing equipment, and to provide an o
Checkpoint equipment	37,000	37,000		(113)	459		(7,900)	30,346		30,346	
Electronic Surveillance	14,000	14,000		(38)	153		(4,000)	10,115		10,115	
Maintenance for Chkpt Equip.	31,000	31,000		(113)	480		3,633	35,000		35,000	The Sept. 11th Commission recommended that TSA take immediate action to improve explosives screening of all higher risk passengers at airport screening checkpoints. TSA will invest $100M between FY05 & FY06 for emerging checkpoint explosives technology.
Emerging Technology	28,300	28,300						28,300	43,700	72,000	
4 Secure Flight	**34,922**	**34,919**				(34,919)					
5 Crew Vetting	**10,038**	**10,000**				(10,000)					
6 Registered Traveler Program	**15,099**	**15,000**				(15,000)					Transfer to SCO
7 EDS/ETD Systems	**609,839**	**399,940**						**367,000**		**367,000**	
EDS/ETD Purchase	180,104	180,000		(563)	2,297		(51,734)	130,000		130,000	FY06 adjustments based on: maintaining LOI reimbursement levels at 75% and 90% for large and smaller airports, respectively, and the elimination of Aviation Security Capital Fund formula distribution requirements; fewer purchases of equipment required f

	FY2005 Proposed Spendplan	FY 2005 Enacted	Annualization of FY 05 Pay	Efficiency[1]	PAY/ NON PAY	Xfer Out	Remix & Program Decreases	Total FY 06 Base	Passback/Final Appeals Apprvd	Total	Comments
EDS/ETD Install	249,534	45,000					(31,000)	14,000		14,000	
EDS/ETD Maintenance/Utilities	180,201	174,940		(657)	2,679		23,038	200,000		200,000	
Operational Intergration						23,000		23,000		23,000	
Sub-Total Screening Operations	**3,790,582**	**3,501,633**	**11,174**	**(12,848)**	**77,121**	**(36,919)**	**(101,913)**	**3,438,248**	**223,681**	**3,661,929**	
B Aviation Direction & Enforcement											
1 **Aviation regulation & other**	**225,601**	**230,000**						**232,196**		**238,196**	
K-9 Units	20,000	20,000	83	(56)	260		(1,200)	19,087		19,087	In order to balance competing requirements within the budget, TSA will maintain K-9 efforts slightly below FY05 level to provide an offset for screener pay and benefits, human resources (HR) services, and information technology.
State and local	70,000	70,000		(263)	1,072			70,809		70,809	
Airport regulation & inspections	135,601	140,000	682	(525)	2,143			142,300	6,000	148,300	Increase funding by $6M and 31 FTE for foreign and domestic repair station inspection operations to meet the requirements of Vision 100 - Century of Aviation Reauthorization Act - and ensure that Foreign and Domestic Repair Stations are inspected.
2 **Airport mgmt, IT & Support**	**666,382**	**526,890**						**584,370**		**758,370**	
Airport Management and Staff	270,000	284,000	1,383	(1,089)	4,348		(9,000)	279,662		279,662	
Airport Rent and Furniture	100,000	100,000		(375)	1,531			101,156		101,156	
Airport Parking & Transit Benefits	15,890	15,890		(56)	243			16,077		16,077	
Airport Staff Info Tech	143,300	85,000		(413)	1,684		81,070	167,341		167,341	This increase of 81.07M is an adjustment to accurately reflect IT's base and align it with the assumptions in the FY 2005 reprogramming request.
HI Soc Initiative									174,000	174,000	$174M completes the installation of HI-SOC connectivity TSA-wide.
Sabre	20,192	25,000		(94)	383		(22,369)	2,930		2,930	Sabre development complete. Reduction represents investment costs no longer required to create the screener scheduling information system. TSA will retain operating funds to maintain system in FY06 and the outyears.
Transportation Security Coordination Center	17,000	17,000		(56)	260			17,204		17,204	
3 **Flight Crew Training**	**27,000**	**25,000**						**25,289**		**35,289**	
Federal Flight Deck Officers	25,000	25,000		(94)	383			25,289	7,000	32,289	The $7M increase is required to recertify and requalify the current FFDO population while continuing to meet the demand for addition FFDOs.
Crew Member Self Defense	2,000								4,000	4,000	To provide for the first full year of the voluntary self-defense training program for flight and cabin crewmembers.
4 **Air Cargo**	**43,365**	**40,000**	146	(113)	459		(492)	**40,000**		**40,000**	
Sub- total Aviation Direction & Enforcement	**862,348**	**821,890**	**2,294**	**(3,114)**	**12,766**		**48,019**	**881,855**	**191,000**	**1,072,855**	
Sub-total - Aviation Security	4,652,930	4,323,523	13,468	(15,962)	89,887	(36,919)	(53,894)	4,320,103	414,681	4,734,784	

EMERGING CHECKPOINT EXPLOSIVES TECHNOLOGY

Question. For fiscal years 2005 and 2006, provide a deployment schedule, including the identification and cost of the technology acquired, the manufacturer of the technology, and the airports at which the technology has been or will be deployed.

Answer. The following list of airports (Fig. 1) will have checkpoint Explosives Detection Trace Portals deployed by January 2006. TSA is deploying the systems concurrently, therefore the list does not reflect any sort of priority. The timing for deployment between now through January 2006 will depend on the results of site surveys that are currently underway and the production capabilities of the vendor.

TSA will be purchasing two different portals, the GE Ion Track Entry Scan and the Smiths Sentinel, and the results of the site surveys will help TSA determine which of the two technologies is best suited for each of the airports listed. TSA is planning to purchase equal numbers of each of the two products.

In fiscal year 2005, TSA received $28.3 million to field emerging technology equipment at checkpoints. For fiscal year 2006, TSA is requesting a total of $72 million (an increase of $43.7 million over the fiscal year 2005 base amount) for emerging checkpoint explosives technology.

In support of checked baggage screening, the following list of airports (Fig. 2) will have the Reveal Technologies CT–80 deployed by January 2006. Like the checkpoint Explosives Trace Detection Portal, TSA's intent is to deploy the CT–80s concurrently, therefore this list does not reflect any sort of priority. The timing for deployment between now through January 2006 will depend on the results of site surveys that are currently underway and the production capabilities of the vendor. Consistent with the direction provided in the Homeland Security Appropriations Act, 2005, $30 million will be spent for purchase and installation of this capability.

FIG.1—EXPLOSIVES DETECTION TRACE PORTALS

	Airport
ATL	Hartsfield-Jackson Atlanta International
BOS	Boston Logan International
BWI	Baltimore/Washington International
CLE	Cleveland-Hopkins International
CLT	Charlotte/Douglas International
CMH	Port Columbus International
CVG	Cincinnati/Northern Kentucky International
DCA	Ronald Reagan Washington National
DEN	Denver International
DFW	Dallas/Ft. Worth International
DTW	Detroit Metropolitan Wayne County
EWR	Newark Liberty International
FLL	Fort Lauderdale/Hollywood International
HNL	Honolulu International
IAD	Washington Dulles International
IAH	Houston Intercontinental
IND	Indianapolis International
JFK	John F. Kennedy International
LAS	McCarran International
LAX	Los Angeles International
LGA	LaGuardia International
MCI	Kansas City International
MCO	Orlando International
MDW	Chicago Midway International
MIA	Miami International
MSP	Minneapolis-St. Paul International
OAK	Metropolitan Oakland International
ORD	Chicago O'Hare International
PBI	Palm Beach International
PDX	Portland International
PHL	Philadelphia International
PHX	Phoenix/Sky Harbor International
PIT	Pittsburgh International
RDU	Raleigh-Durham International
SEA	Seattle-Tacoma International
SFO	San Francisco International
SJU	Luis Munoz Marin International

FIG.1—EXPLOSIVES DETECTION TRACE PORTALS—Continued

	Airport
SMF	Sacramento International
SNA	John Wayne Airport-Orange County
STL	Lambert-St. Louis International
TPA	Tampa International

FIGURE 2.—REVEAL TECHNOLOGIES CT–80

	Airport
ABE	Lehigh Valley International
ACY	Atlantic City International
ALB	Albany International
BGR	Bangor International
BIL	Billings Logan International
BTV	Burlington International
CHS	Charleston AFB/International
ELP	El Paso International
EYW	Key West International
FAI	Fairbanks International
GPT	Gulfport-Biloxi International
GSP	Greenville-Spartanburg International
HGR	Hagerstown Regional-Richard A Henson Field
HPN	Westchester County
HSV	Huntsville International-Carl T Jones Field
ISP	Long Island MacArthur
LGB	Long Beach/Daugherty Field
MRY	Monterey Peninsula
OMA	Eppley Airfield
ORF	Norfolk International
PIE	St. Petersburg-Clearwater International
RNO	Reno/Tahoe International
ROC	Greater Rochester International
SWF	Stewart International
SYR	Syracuse Hancock International
TYS	McGhee Tyson

Question. Has the checkpoint technology that has been deployed been verified by the Science & Technology Directorate?

Answer. TSA works closely with the S&T Directorate and discusses its ongoing R&D efforts to ensure the S&T Directorate is not only aware of but supports TSA's efforts related to technology development.

HAZARDOUS MATERIALS ENDORSEMENT FOR COMMERICAL DRIVER'S LICENSE

Question. On January 13, 2005 a final rule was published in the Federal Register which established a fee for individuals who apply for or renew a hazardous materials endorsement for a commercial driver's license. According to the final rule, TSA intends to use fees collected under this rule to pay for the costs of the security threat assessments and the costs of collection and transmission of finger prints and biographical information.

Please provide the committee with an estimate of the amount of money these new fees are expected to bring in.

Answer. By law, the fees for individuals who apply for or renew a hazardous materials endorsement for a commercial driver's license cannot be collected in excess of the expenses to run the program. Accordingly, the program is expected to cost about $9 million in fiscal year 2005 and approximately $28 million in fiscal year 2006. The original fiscal year 2006 estimate of $44 million was adjusted mainly due to the change in the estimated HAZMAT applicant population.

PRIVATE SCREENERS

Question. The budget proposes an increase of $15 million to continue the privatized screening contracts at the current service levels. Explain why an additional $15 million is necessary when, currently, only one airport has applied for a

private screening workforce. Does TSA still anticipate the current number of airports participating in privatized screening contracts to remain the same?

Answer. As of May 2005, the Screening Partnership Program (SPP) had received a total of seven applications, which includes the original contract screening pilot program (PP5) airports (San Francisco, Kansas City, Rochester, Jackson Hole and Tupelo), and two new airports (Elko, Nevada and Sioux Falls, South Dakota).

In directing TSA to establish PP5, ATSA required that the level of screening services and protection provided at the PP5 airports be equal to or greater than the level provided at an airport with Federal screeners. Similarly, contract screeners must receive compensation and other benefits that are not less than the compensation and other benefits provided to Federal personnel. In accordance with these requirements, TSA strives for a level playing field between airports with private contract screeners under PP5 and the SPP and airports with Federal screeners. Consequently, as each airport considers whether to continue with Federal screening or to apply for the SPP, it can base its decision on its own preferences and criteria rather than considerations of security, resources, or level or service.

The additional $15 million requested is reflective of the increased cost of providing screening services at the levels required under ATSA. TSA is not funding services in addition to those provided in previous years except where consistent with changes in the Standard Operating Procedure made effective throughout the Nation's commercial aviation system.

In fiscal year 2005, a reprogramming increase of $23 million was made to support the cost of providing PP5 airports with the level of screening required for all commercial airports under ATSA. This reprogramming supported increased insurance premium costs for worker's compensation, terrorism and health insurance premiums, ATSA-guaranteed screener pay parity, and operational requirements relating to flexibilities granted to contractors in the areas of recruitment, hiring, and training.

Question. Are any of the airports currently participating planning or considering opting out of the private screening program?

Answer. TSA has received applications from all five private screening pilot airports to participate in the SPP.

Question. Are other airports not currently participating in the program planning to opt in?

Answer. While several airports have expressed interest to TSA about participating in the SPP, to date, only Elko Regional Airport and Sioux Falls Regional Airport have formally applied.

FOREIGN AND DOMESTIC REPAIR STATION INSPECTIONS

Question. The budget request includes $6 million for Foreign and Domestic Repair Station Inspection Operations. Does TSA have a schedule to inspect the 664 Foreign and Domestic Repair Stations? If so, provide the schedule to the Committee.

Answer. TSA has developed a Notice of Proposed Rulemaking (NPRM) that will increase security at both foreign and domestic repair stations. The NPRM is currently under Departmental review and is expected to be released for public comment in late summer of 2005. The agency has not yet developed a firm schedule for auditing all foreign repair stations. TSA is currently developing a survey document that will be sent to repair stations to assess their operations. This effort will assist in determining which repair stations pose the greatest potential risk and should be given priority for audits. TSA is also developing the necessary assessment tools for use by the inspectors during their visits to repair stations.

TSA fully expects to have developed the assessment tools necessary for the auditing effort by the time the final rule for repair station security is released, which TSA expects to occur by spring 2006. The actual schedule of audits will be dependent upon the initial survey of repair stations, which will begin as soon as the final rule is released.

Question. Is $6 million and 31 FTE the full amount necessary to inspect all Foreign and Domestic Repair Stations and the domestic maintenance, repair and overhaul facilities in the United States? If not, how much is needed to comply with "Vision 100?"

Answer. TSA would like to note that the $6 million and 31 FTE are earmarked solely for audits of foreign repair stations, of which there are approximately 650. There are approximately 4,500 repair stations in the United States, and current plans are to cover domestic audits with the existing force of Aviation Security Inspectors (ASI). Approximately 950 ASIs are presently assigned to geographical areas across the United States and inspect all facets of regulated aviation assets, not just repair stations.

The hiring projection with the $6 million requested in the fiscal year 2006 Budget is 12 inspectors, one program manager, and one program analyst. It is anticipated that additional foreign repair station inspectors, plus a manager and analyst, will be hired over a three-year time period. The hiring and operating projection costs of the program for its second and third years will be more accurately approximated after TSA assesses the costs of the initial year of the program.

TSA R&D

Question. The budget proposes to consolidate TSA R&D activities within the Science and Technology (S&T) Directorate. However, only $109 million is proposed for fiscal year 2006 within the S&T budget. TSA's budget maintains $23 million for operation R&D activities, such as pilot projects. Please explain why the program is proposed to be cut by $46 million and what impact that would have on ongoing R&D activities and those planned prior to the transfer proposal.

Answer. The $46 million consists of the following reductions: $25 million from Air Cargo R&D and $21 million from Explosives Detection Equipment (EDS) R&D. The reductions are appropriate given maturing technology in both areas, which, for example, will result in the deployment of Explosive Detection Trace Portals to 41 airports by the end of January 2006.

Overall, the reductions will have minimal effect on the R&D activities that would have been undertaken by TSA because those activities were budgeted by TSA and included in the proposed amount of $109 million.

REGISTERED TRAVELER

Question. Last year, TSA indicated that, assuming there was sufficient national interest in the program, the $15 million provided in fiscal year 2005 would be used for start-up operational costs and future funding would be generated by fees incurred by participants. What is the amount anticipated in fiscal year 2006 from offsetting collections?

Answer. TSA envisions a fully operational RT Pilot Program to be fee funded. The President's fiscal year 2006 Budget proposal includes $22.5 million from potential offsetting collections for RT, which was consolidated into the proposed SCO. However, TSA will need to implement a fee rule to accept fees for RT.

Question. What is the timeline and deployment schedule for implementing this program beyond the pilot stage?

Answer. Through a series of concurrent stand-alone pilots, TSA has been aggressively testing the RT concept of running threat assessment and identity verification checks on eligible volunteers in order to provide them with an expedited clearance through security checkpoints. TSA is currently running successful programs at five Federally managed pilot sites (Minneapolis, Los Angeles, Houston, Boston, and Washington, D.C.), which are scheduled to be completed in September 2005. TSA is concurrently working with the GOAA to launch a sub-pilot at Orlando International Airport in summer 2005 that will assess the feasibility of incorporating a private sector component into the RT concept.

Results of these pilots will be analyzed to determine the program's effect on security and service, enabling the Department to make decisions about full scale implementation of RT. Any timeline and deployment schedule for implementing RT beyond the pilot stage will be linked to the Department's decision.

DEEPWATER BUDGET

Question. Virtually the entire increase requested for Deepwater in fiscal year 2006 is just to sustain legacy assets. The revised Deepwater plan indicates that the lifecycle costs to sustain legacy assets could cost anywhere between $828 million and $1.8 billion. Why is there such a large difference between these two amounts?

Answer. The difference the two amounts is a function of time and money. The lower number reflects a lower total acquisition cost ($19 billion) over a shorter implementation period (20 years). The higher legacy asset funding amount reflects a higher total acquisition cost ($24 billion) over a longer implementation period (25 years). The shorter plan invests less funding in legacy sustainment, decommissions legacy assets sooner, but commissions fewer new assets. The longer plan invests more in legacy sustainment to keep the assets in commission longer, invests more in technology refresh/obsolescence prevention (i.e. life cycle costs), and delivers more new assets. Earlier decommissioning of legacy assets translates into lower legacy sustainment costs, but equates to a lower number of assets to perform Coast Guard missions both during build out and upon completion.

Question. What is the Coast Guard doing to better plan and prepare for legacy asset sustainment?

Answer. The Coast Guard has a detailed plan for maintaining its legacy cutters and aircraft. Coast Guard men and women are well trained to maintain and continually upgrade Coast Guard aviation, surface, and shore infrastructure assets. A mature project planning and execution program exists within the Coast Guard to provide routine unit-level and depot-level maintenance. Where expertise or infrastructure doesn't exist organically within the service, the Coast Guard uses contracted resources to provide the requisite maintenance support. Maintaining a high proficiency level amongst the Coast Guard's "maintainers" is critical to the long-term health of the service. One of the service's guiding principles is to maintain a core competency of maintenance expertise amongst Coast Guard (military and civilian) members to ensure service readiness, especially during periods of national emergency.

The Coast Guard maintains its legacy aircraft and vessels using organic maintenance and repair infrastructure in conjunction with contracted depot-level maintenance activities. These operating expense (OE) funded maintenance efforts are complemented by periodic Acquisition, Construction and Improvement (AC&I) projects which either enhance/sustain asset capabilities and extend asset service lives, or replace assets.

On April 20, 2005, the Coast Guard submitted a legacy asset report to Congress, detailing the Coast Guard's legacy asset issues. This report reflects legacy cutter and aviation AC&I projects that the Coast Guard has included in the fiscal year 2006 Budget request and anticipates requesting in future budget submissions.

Question. The Coast Guard's capital investment plan indicates that the Deepwater budget will be decreased by $214 million in fiscal year 2007. How can you propose such a cut in light of increasing mission demands and the "declining readiness" of existing assets?

Answer. The President's fiscal year 2006 Budget requests $966 million for Deepwater, $242 million above the fiscal year 2005 enacted levels, to fund critical modernization initiatives such as production of the third National Security Cutter and design and long lead material purchase for the Offshore Patrol Cutter while addressing immediate legacy asset issues such as HH–65 re-engining and Medium Endurance Cutter mission effectiveness programs. The Coast Guard's fiscal year 2006–2010 Capital Investment Plan contains $752 million for Deepwater in 2007 to highlight the one-time nature of several of these investments in legacy asset conversions and sustainment projects.

Question. The GAO recently testified that the Coast Guard has acknowledged that it needs to develop condition measures that more clearly demonstrate the extent to which asset conditions affect mission capabilities, but such measures have not been finalized or implemented. What is the Coast Guard's schedule for putting such measures in place?

Answer. To track the condition of the its cutters, the Coast Guard currently measures a Percent of Time Free (POTF) of major casualties measure that shows the general decline in condition of Deepwater legacy assets between 2000 and 2004. To track the condition of the its aircraft, the Coast Guard currently measures aircraft availability rates. However, as GAO has pointed out, "the Coast Guard's available condition measures are inadequate to capture the full extent of the decline in the condition of deepwater assets with any degree of precision." and Justice Issues, testified to the House Committee on Transportation and Infrastructure that, "Other evidence we gathered, such as information from discussions with maintenance personnel, point to conditions that may be more severe than the available measures indicate."

The Coast Guard acknowledges that it needs better condition measures to more accurately depict the condition of its assets. To address this issue, the Coast Guard is developing condition measures that more clearly link cutter condition to mission capability. This effort is scheduled for completion by the end of fiscal year 2005.

In fiscal year 2004, a team of personnel was assembled from engineering support activities in both Atlantic and Pacific Areas to work with Coast Guard Headquarters to construct an asset condition matrix that incorporates engineering casualty reporting (CASREP) data and performance data maintained in the Coast Guard's Readiness Management System (RMS). To do so, the team is identifying/linking thousands of shipboard engineering subsystems across every cutter class and their direct impact/contribution to each Coast Guard mission.

By establishing a clear relationship between engineering subsystems and mission performance, the Coast Guard will be better able to identify return on its maintenance investments and determine the best use of limited maintenance resources.

The Coast Guard is currently working to develop a comparable measure for its aviation assets; however, it has not established a timeline for implementation.

Question. The GAO report also noted that certain legacy costs, such as maintaining the 378-foot class through 2016 instead of 2013 as originally planned, is not addressed in the revised Deepwater budget baseline. How much funding will this require and are there other legacy assets that need further maintenance but are not included in the revised Deepwater plan?

Answer. Legacy asset sustainment is a Coast Guard stewardship priority that requires judicious balancing of current and future demands on limited AC&I investment resources. One of the primary determining factors is how long the asset class will remain in service. The 378-foot High Endurance Cutters (WHEC) are the first legacy cutters expected to be removed from service as the National Security Cutters (NSCs) are deployed. Therefore, the Department and the Coast Guard have invested AC&I funds toward acquisition of NSCs vice sustaining WHECs. Until they are decommissioned, WHECs will be sustained through routine depot level maintenance funded within the Coast Guard's Operating Expense Appropriation. The 210-foot and 270-foot medium endurance cutters are projected to remain in service longer, therefore substantial AC&I investments are being made in these classes in the form of Mission Effectiveness Program funds sought in fiscal year 2006 and in the outyears. Similar legacy sustaining initiatives are funded in the Deepwater implementation plan for aircraft that will remain in the Coast Guard's final Deepwater inventory. Additional details on the Coast Guard's plan to sustain its legacy assets are provided in a report that was submitted to Congress on April 20, 2005.

Question. What measures have the Coast Guard put in place to ensure that competition is built into Deepwater acquisition decisions?

Answer. From the beginning of the acquisition process, the Coast Guard has ensured competition has been built into the Deepwater program. The GAO recently reported that all assets originally planned for the first five years of the contract were properly competed through the initial contract award process that resulted in selection of Integrated Coast Guard Systems (ICGS) as the Deepwater contractor. Beyond the initial contract award process, the Coast Guard has taken several steps, including implementing GAO recommendations to ensure acquisitions decisions are adequately competed. There are many examples of competition in subcontracts that can be provided, if desired. For example, where changes to the original proposal have been introduced into the acquisition, the Coast Guard ensures that a competitive price determination is made. The price of this change order must be determined to be fair and reasonable before the Coast Guard will approve ICGS action. The Coast Guard monitors ICGS' use of the open business model as required by their internal procedures for second-tier subcontractors. ICGS also requires the first-tier subcontractors to encourage 2nd and 3rd tier suppliers to promote competition.

Question. What is the cost comparison of re-engining the existing fleet of HH–65 aircraft versus the procurement of a new aircraft outfitted to perform the same mission?

Answer. Re-enginging an HH–65 helicopter costs approximately $3 million. It would cost approximately $19 million to buy a new, commercial aircraft capable of performing the missions of a re-engined HH–65. Under the revised Deepwater implementation plan, HH–65 helicopters will receive additional upgrades to become multi-mission, cutter helicopters. The total cost of the re-engining and the upgrade to Multi-Mission Cutter Helicopter (MCH) is slightly less than $7 million per unit. To replace the entire HH–65 fleet would cost $1.8 billion vice $636 million for upgraded HH–65s, three times as much. It should also be noted that when the Coast Guard made the decision to re-engine the HH–65s it was in the face of a crisis in engine safety and reliability. Timely resolution of that crisis did not allow for acquisition of a replacement fleet. Further, HH–65 re-engining was already planned as part of the Deepwater solution. Re-engining was the most timely, cost-effective short and long-term solution.

Question. What is the status of the HH–65 re-engining process?

Answer. In August 2004, the first re-engined HH–65 was delivered to the Coast Guard at Aviation Training Center Mobile, AL, for operational testing and evaluation. As of the first of September 2005, 10 re-engined HH–65Cs had been delivered for full operational status to Air Station Atlantic City, NJ, (5), Aviation Training Center Mobile, AL, (1), and Air Station Savannah, GA, (4). To accelerate the HH–65 re-engining project the Coast Guard and its contractor, Integrated Coast Guard Systems (ICGS), have examined the quality and suitability of a second re-engining facility located in Columbus, MS. In August 2005, this facility delivered its first re-engined aircraft to the Coast Guard. This aircraft was determined to meet needed quality and suitability parameters and the Coast Guard contracted with ICGS to re-engine an additional 11 aircraft at the Columbus facility. The Coast Guard plans to have all 84 operational aircraft re-engined in early 2007.

Question. Will the 24 month schedule be met?

Answer. Provided the President's fiscal year 2006 request of $133.1 million for HH–65 re-engining is fully funded, the Coast Guard's plan is to complete re-engining the operational fleet of 84 helicopters by February 2007. This is the fastest possible production schedule based on the availability of engine kits and parts, maximum production at Coast Guard Aviation Repair and Supply Center, additional production capacity that may become available at a second facility, and number of aircraft that can be removed from operational service at any given time.

Question. What is the current timetable?

Answer. The first re-engined HH–65 was delivered for operational test and evaluation in August 2004. Regular production delivery of operational HH–65 began in April 2005, when the second HH–65 was returned to operational status at Air Station Atlantic City, NJ. Four others are scheduled for delivery in May 2005. In fiscal year 2005, a total of 29 conversion starts are planned. In fiscal year 2006, 51 conversion starts are planned. All 84 operational aircraft are scheduled for completion early in fiscal year 2007. Re-engining of all 95 HH–65s is scheduled to be completed in 2007.

Question. What barriers exist that could the Coast Guard from meeting this schedule?

Answer. The current timetable, resulting in completing the re-engining of the Coast Guard's operational fleet of 84 HH–65 helicopters, is based on the best outcome of a number of variables. To achieve this schedule there must be:

—Full support of the President's Budget request for $133.1 million in fiscal year 2006 funding for re-engining;
—Maximum availability of engine kits and parts;
—Effective mitigation of operational needs to maximize the number of aircraft that can be removed from operational service at any given time;
—The highest possible production at Coast Guard Aviation Repair and Supply Center; and
—Additional production capacity at a second facility.

If any of these variables are not optimal, then the schedule will not be met.

DEEPWATER PROGRAM MANAGEMENT

Question. For fiscal years 2005 and 2006, provide a detailed spend plan for program costs for ICGS Management and Government program management/ICGS.

Answer.

SYSTEMS ENGINEERING & INTEGRATION BUDGET

[Dollars in millions]

Activity	Fiscal year 2005	Fiscal year 2006
Systems Engineering:		
Performance Engineering (Measurement & Modeling) [1]	6	6
Engineering and Process Management [2]	15	16
Integration Management:		
Systems Operations Management [3]	17	17
Data Management [4]	2	2
Award Fee Pool	3	
Total	43	45

[1] *Performance Engineering.*—In accordance with Deepwater's performance-based acquisition, Performance Engineering includes the efforts required to measure the degree to which the Integrated Deepwater System achieves the overarching goals of maintaining and improving operational performance while managing total ownership costs within an aggressive baseline. Risk reduction is achieved through modeling, simulation, and analysis coupled with test & evaluation to assess the appropriate mix and capabilities of Deepwater assets to achieve the desired operational performance.

[2] *Engineering and Process Management.*—Engineering Management consists of the overarching technical management team responsible for translating Coast Guard operational and performance requirements into a cohesive Implementation Plan and managing all the technical efforts required to develop, deliver, deploy, and maintain the Deepwater assets critical to achieving the Implementation Plan. Correspondingly, Process Management is responsible for leading the identification, evaluation, implementation and improvement of Deepwater technical engineering processes deemed critical to the successful execution of the Implementation Plan.

[3] *Systems Operations Management.*—The Systems Operations Management effort includes the industry program management tasks required to direct and control all organizational functions including engineering, business management, contract management, quality management, configuration management, and data management. An Integrated Deepwater System Program Management Team (including C4ISR, Surface, Aviation, and Integrated Logistic Systems management teams) ensures effective cost control, schedule, and technical performance required to maintain the System-Of-Systems approach necessary for the Coast Guard to perform its specified missions.

[4] *Data Management.*—The Data Management effort includes tasks required to provide configuration control infrastructure for all data across the program. A program-wide Integrated Product Data Environment is utilized to integrate the efforts of geographically-separated engineering teams using a common toolset to enable rapid collaboration and sharing of consistent information.

Deepwater Program management funds are used for technical support from private sector and other government agencies not available within the Coast Guard.

GOVERNMENT PROGRAM MANAGEMENT BUDGET

[Dollars in millions]

Activity	Fiscal year 2005	Fiscal year 2006
Technical Performance Support:		
Technical Engineering Support [1]	19.1	20.1
Operational Tests and Evaluation [2]	3.8	4.0
Program Management Support:		
Financial Management [3]	3.0	3.1
Transition Support [4]	4.6	4.9
Management Support [5]	2.6	2.7
Performance Metrics/Measurement Support [6]	2.2	2.3
Information Technology [7]	2.7	2.9
TOTAL	38.0	40.0

[1] *Technical Engineering Support.*—Aeronautical, electronics and naval engineering; logistic systems, Command and Control, weapons system certification, and other expertise not available from Coast Guard resources.

[2] *Operational Tests and Evaluation.*—Navy's Commander Operational Test and Evaluation Forces is the technical advisor to the Coast Guard responsible for management of independent tests for the early review and assessment of Integrated Deepwater System asset operational performance.

[3] *Financial Management.*—Includes independent analysis and support of the Defense Contract Auditing Agency, other Defense Contract support, performance/risk management, financial systems management provided to asset level Program Management Representative Offices for independent cost analysis and pricing.

[4] *Transition Support.*—Augments Coast Guard teams for delivery of new assets, existing infrastructure changes, developing document configuration and management, graphics support, and support for training infrastructure analysis, manpower analysis, operations doctrine development, architecture analysis.

[5] *Management Support.*—Provides for program specific training, project management and outreach initiatives as recommended by Government Accountability Office.

[6] *Performance Metrics/Measurement Support.*—Modeling, simulation, and analysis of various inputs to include Total Ownership Cost, Operational Performance, and Earned Value Management Processes.

[7] *Information Technology.*—Specialized information technology to support Deepwater Program management.

MARITIME TRANSPORTATION SECURITY ACT IMPLEMENTATION

Question. On July 1, 2004, port facilities and vessels were required to submit security plans to the Coast Guard and to be in compliance with those plans. The Coast Guard has now inspected approximately 2,900 regulated facilities. The Government Accountability Office (GAO) recently concluded that it is unclear if the Coast Guard's inspection process has been effective or not. Can you describe what the Coast Guard is doing to ensure that these facilities are following through on their security plans?

Answer. The Coast Guard ensures that facilities operate in accordance with their approved security plans through annual exams and spot checks. The Coast Guard continues to work constructively with GAO to insure Coast Guard requirements and procedures are sustainable and that they make a positive impact on the security of the maritime transportation system. The requirement for an evaluation of vessel and facility security plans is one tool to reduce vulnerabilities in this critical system—the vast majority of which is owned and operated by the private sector. To ensure that regulatory and inspection frameworks continue to serve the intended objectives, regular evaluations and performance metrics are being developed to assess their effectiveness. For example, the Coast Guard plans to begin an evaluation of its facility inspection efforts in June 2005, complete the field portion of the evaluation in September 2005, and produce a final evaluation in December 2005.

Question. Last year, GAO reported that many facility and vessel owners said it would be difficult to obtain the financial resources to fully mitigate their known vulnerabilities. GAO reported that one official at a major port indicated that some security vulnerabilities were not included in its facility plan because funding was not available to address them. What is the Coast Guard doing to ensure that the inspection process is just not a "paper exercise" and one that addresses vulnerabilities?

Answer. The Coast Guard has several policies in place that provide for a meaningful inspection process and ensure facilities fully address vulnerabilities.

Prior to final Facility Security Plan (FSP) approval, Coast Guard Captains of the Port review and evaluate each submitted Facility Security Assessment (FSA), ensuring the FSPs identify and addressed all vulnerabilities. This evaluation includes an on-site survey by the Coast Guard.

After approving the FSP, the Coast Guard annually inspects each facility for MTSA compliance. The Coast Guard developed specific inspection policies to ensure that:

—The facility complies with its FSP;

—The approved FSP adequately addresses the performance-based criteria outlined in the regulations;
—The adequacy of the FSA and the Facility Vulnerability and Security Measures Summary (CG–6025); and
—Measures in place adequately address the vulnerabilities.

To carry out the inspections, qualified Coast Guard facility inspectors use a published, comprehensive inspection guide to identify deficiencies and any vulnerability not previously disclosed.

Question. With no port security grant program, how can ports know that resources are available to implement the MTSA?

Answer. DHS has administered a total of four port security grant rounds since fiscal year 2002. The Coast Guard has played a significant role in all four grant rounds, participating at every step of the process, from field recommendations to the grant awards—which have totaled over $560 million since September 11, 2001.

In 2004, Secretary Ridge designated the Office of State and Local Government Coordination and Preparedness (SLGCP) as the Department's "one-stop shop" to centralize State and local terrorism preparedness and grant administration with other emergency preparedness grant programs, including the Port Security Grant Program previously administered by the TSA. The centralization will provide better service to key stakeholders and provide a more effective overall homeland security grant program. The Coast Guard will maintain an important and active role in the port security grant process. $150 million was appropriated for fiscal year 2005 (Round 5) port security grants. A fact sheet regarding round 5 is available upon request. Additional information on the port security grant program can be found at the following internet address:

https://www.portsecuritygrants.dottsa.net/TSAdotnet/default.aspx

REQUIREMENTS GAP

Question. The Coast Guard's budget references a July 2004 "Call to Action" from the U.S. Interdiction Coordinator. That report noted that actionable intelligence has never been better but the United States is frequently unable to pursue identified interdiction opportunities. An example of this is the amount of operational hours that are available for the Coast Guard's Maritime Patrol Aircraft.

To meet the operational requirements cited in the Coast Guard's MPA requirements study, the Coast Guard would have to double the amount of maritime patrols from the current capability of 32,000 hours. Your budget includes an increase of only 1,500 maritime patrol hours for homeland security, counter-drug, and other mission areas. Why does such a large gap in requirements exist and what will it take to close it?

Answer. The Coast Guard fixed wing requirements were determined by calculating the post-September 11 mission needs above the 1998 Coast Guard multi-mission baseline. The 1998 baseline was 44,400 hours. The additions are: 5,139 hours for counter-drug (CD) hours based on Joint Inter-Agency Task Force South analysis of the Department of Defense and multi-national drawdown in CD forces; 18,195 hours for maritime security long range surveillance under moderate, high and imminent threat periods; and 285 hours for Coast Guard Strike Force and Maritime Safety and Security Team transport. Given that 32,400 flight hours are available from Coast Guard fixed wing aircraft in fiscal year 2005, this leaves a gap of 34,454 hours.

The Coast Guard's fiscal year 2006 budget includes several initiatives to help mitigate the current Maritime Patrol Aircraft (MPA) shortfall:

—$16.5 million is requested for C–130H augments, providing an additional 1,500 annual C–130H MPA flight hours. Funding will also provide for dedicated aviation sensor personnel and enhanced sensors to improve effectiveness in high-threat zones, and permanently establish forward operating and logistics support for MPA operating in the Central/South American region to maximize time "on station" and reduce aircraft downtime due to unscheduled maintenance.
—$12.6 million is requested for 1200 additional annual operations flight hours for C–130Js to conduct proficiency training and logistics flights—freeing up missionized C–130Hs to conduct MPA missions.
—$5 million is requested to continue the missionization of the 6 C–130Js, through operation of the Aircraft Project Office, which are estimated to be completely missionized by 2008.
—$8.7 million is requested to staff and support the first two CASA aircraft in advance of delivery and full operating capability anticipated in 2007.

The MPA gap will likely persist until the Deepwater system (including the CASAs, C–130s, and unmanned aerial vehicles) is fully built out.

Question. What other major Coast Guard assets have a gap between capabilities and mission requirements?

Answer. The significant capability gaps faced by the Coast Guard's major assets in the post-September 11 environment were the catalyst for the Deepwater Performance Gap Analysis and subsequent Mission Need Statement and the revised Deepwater Implementation Plan. These gaps are quantified both under capability—the attributes of individual assets, and capacity—force structure/fleet size. The following table depicts the capabilities and capacity for the Deepwater fleet to begin to close these gaps.

In addition to the MPA gap, a capacity gap exists with the patrol boat fleet. Considering available 110-foot and 123-foot patrol boats and 179-foot patrol coastals on loan from the U.S. Navy, total patrol boat available hours reached it lowest point of approximately 75,000 in 2004. This is considerably lower than the 1998 baseline of approximately 100,000 hours, and is a result of having cutters deployed to Operation Iraqi Freedom, and cutters out of service for the 110–123 foot conversion program. With the advancement of the fast response cutter design and construction, the Coast Guard should reach the 1998 baseline again between 2013 and 2015.

	Original Mission Needs		Revised Mission Needs	
Asset	Fleet Size	Capabilities	Fleet Size	Capabilities
National Security Cutter (NSC)/Maritime Security Cutter, Large (WMSL)	8	Deepwater Interoperability	8	DHS/DOD/Rescue 21 (R21) Interoperability
		Basic CG Command and Control (C2) Feed		Remote/Integrated Anti-Terrorism/Force Protection (AT/FP) Weapons
		Forward Looking Infrared		Redundant/Hardened/Improved C2
				Underwater Detection
Offshore Patrol Cutter (OPC)/Maritime Security Cutter, Medium (WMSM)	25	Deepwater Interoperability	25	DHS/DOD/R21 Interoperability
		22 kt Speed		CG COP Connectivity
		Standard Flight Deck		
				Integrated Electo-Optical/Infrared System
	....	Threat Receiver	....	Chemical, Biological, Radiological, Nuclear & Explosive (CBRNE) Detection
		30mm Gun		
		Manual Small Arms		Enhanced Maritime Patrol Surveillance Capability
				Nation-wide DHS Strategic Lift
Fast Response Cutter (OPC)/Maritime Patrol, Coastal (WPC)	58	Deepwater Interoperability	58	DHS/DOD/R21 interoperability
		30mm Gun		Remote Weapons & AT/FP Suite
		Baseline C4 Suite		Redundant, Hardened C4
		Threat Receiver		Defense Survivability
		20-yr Steel Hull		40-yr Composite Hull
				CBRNE Detection & Defense
				Underwater Detection
Short Range Prosecutor (SRP)	42	Deepwater Interoperability	33	DHS/DOD/R21 Interoperability
Long Range Interceptor (LRI)	82	Deepwater Interoperability	91	DHS/DOD/R21 Interoperability
Long Range Surveillance Aircraft (LRS)/ HC–130H/J	6	Deepwater Interoperability	22	DHS/DOD/R21 Interoperability
		Basic CG C2 Feed		CG COP Connectivity
		Forward Looking Infrared		Integrated Electo-Optical/Infrared System
				CBRNE Detection
				Enhanced Maritime Patrol Surveillance Capability
				Nation-wide DHS Strategic Lift
Multi-Mission Cutter Helicopter (MCH)/HH–65C	93	Deepwater Interoperability	95	DHS/DOD/R21 Interoperability
				CG COP Connectivity
				CBRNE Detection
				Airborne Use of Force
				Vertical Insertion/Delivery

Medium Range Surveillance Aircraft (MRS)/CASA CN–235	35	Deepwater Interoperability	36	DHS/DOD/R21 Interoperability CG COP Connectivity Integrated Electo-Optical/Infrared System CBRNE Detection
Medium-Range Recovery Helicopter (MRR)/MH–60T	42	Deepwater Interoperability	42	DHS/DOD/R21 Interoperability CG COP Connectivity Integrated Electo-Optical/Infrared System CBRNE Detection Airborne Use of Force Vertical Insertion/Delivery
Vertical Take-off & Landing UAV (VUAV)	69		45	CBRNE Detection
High Altitude & Endurance UAV (HAEUAV)	7		4	

PORT SECURITY ASSESSMENTS

Question. In the fiscal year 2003 Supplemental, Public Law 108–11, Congress appropriated $38 million to conduct vulnerability assessments at all tier I strategic seaports. Of that amount, $16.8 million remains unobligated. Why hasn't this funding been spent?

Answer. Prior to enactment of Public Law 108–11, the Coast Guard received supplemental funding and was able to conduct Port Security Assessments (PSAs) at 13 of the 55 strategic ports. The average cost of these assessments was $900,000 per port. The $38 million appropriation was to complete remaining port assessments based on this per-port average.

In response to various maritime security initiatives, such as the Maritime Transportation Security Act of 2002, the Coast Guard revised the PSA methodology to ensure that the PSAs provided the greatest value to the port without being redundant to the other initiatives and programs. This updated methodology resulted in a reduction of costs from $900,000 to approximately $300,000 per port.

As of September 14, 2005, the Coast Guard has expended $22.9 million for the completion of PSAs of the Coast Guard's 55 militarily and economically strategic ports, as well as for important port security initiatives such as special technical assessments, development of a Geographic Information System (GIS) viewer, Coast Guard participation in the Comprehensive Review of nuclear power plants, and PSA Program operational costs. The remaining $16.6 million will be expended during the remainder of fiscal year 2005 and 2006 to continue refining port security assessments and our knowledge of port-specific vulnerabilities through specific technical or infrastructure assessments (bridges, tunnels, dangerous cargo, etc.). This additional work is critical to address needs that were identified in the course of the initial port assessments. It will provide important amplifying information to Coast Guard Captains of the Port and the Area Maritime Security Committees allowing them to address effectively port-specific vulnerabilities that have been identified.

Question. How many assessments of tier I ports have been completed to date and what is the schedule to complete all Tier I ports?

Answer. All Tier I PSAs are complete. The Coast Guard has completed PSAs at each of the previously identified 55 militarily and economically strategic U.S. ports, of which "Tier I" ports are a subset.

PORT SECURITY ESTIMATES

Question. Last year, in response to a question for the record on port security, the Committee was told that Department of Homeland Security spending on port security increased by $224 million (13 percent) in the President's Budget, from $1,661 million in 2004 to $1,885 million in 2005. Within the 2005 total is $1,675 million for Coast Guard port, waterway, and coastal security activities, including over $100 million for expenses related to the Maritime Transportation Security Act (MTSA). How was that funding level determined?

Answer. The $1,675 million for Coast Guard Ports, Waterways, and Coastal Security (PWCS) activities in fiscal year 2005 was incorrectly stated in last year's question. The 2005 operating expense budget estimate for PWCS activities estimated in the Coast Guard's 2005 Budget congressional justifications as $1,501 million. The Coast Guard develops estimates of mission-specific spending using an activity based Mission Cost Model. The $101 million increase to implement MTSA attributable to PWCS was included in the $1,501 million estimate.

PORT SECURITY GRANT PROGRAM

Question. The Coast Guard authorization Act for 2005, which was signed into law by the President on August 9, 2004, authorized $35 million for the Secretary to fund pilot programs and award grants to investigate new methods and technologies to better secure our ports. The law specifically cites the need to examine new technologies such as those that can accurately detect explosives, chemical or biological agents, and nuclear materials. The law calls for the examination of new methods for securing our ports such as the use of satellite tracking systems and tools to mitigate the consequences of a transportation security incident. The fiscal year 2006 request does not include funding for this program. What intelligence led the Coast Guard to believe that such a program was unnecessary?

Answer. The Coast Guard is aggressively moving to implement new technologies in order to better secure our ports. Rather than pilot programs or grants, the Coast Guard believes it more prudent in the near term to expend limited resources on the deployment of important proven technologies while other DHS components responsible for development of cross-cutting technologies and private sector grant and re-

search programs administer pilot and grant programs, notably the S&T Directorate and SLGCP. S&T, in particular, has a wealth of research and development expertise as well as an active university research program to pursue technology enhancements across all homeland security requirements. Concurrently, SLGCP is overseeing the administration of a port security grant program that has awarded over $560 million in port security grants already, and will award another $150 million in fiscal year 2005.

In the near term, the Coast Guard is focused on enhancing Maritime Domain Awareness (MDA). MDA is defined as "the effective understanding of anything associated with the global maritime environment that could impact the security, safety, economy or environment of the United States." Effective MDA is a critical enabler to national maritime security strategies and supports the full range of Coast Guard missions.

COVERT SURVEILLANCE AIRCRAFT

Question. What is the Coast Guard's definition of a "covert surveillance aircraft"?

Answer. The 2005 DHS Appropriations Act conference report defines the manned covert surveillance aircraft as a "medium to short range, fixed wing surveillance aircraft." In the context of the Coast Guard's Manned Covert Surveillance Aircraft (MCSA) acquisition project, "covert" is defined as "the capability to operate quietly and surreptitiously enough to enable the surveillance, detection, classification and identification of a maritime target without the target's inhabitants becoming aware of the aircraft's presence."

Question. How will a covert surveillance aircraft serve the Coast Guard's mission?

Answer. The Coast Guard is developing the operational requirements documents that will define the missions and operating parameters for a manned covert surveillance aircraft. The Coast Guard is also examining how this aircraft will fit into the Deepwater system, given that the Deepwater implementation plan accounts for the service-standard fixed, rotary wing and unmanned aircraft necessary to meet projected Coast Guard mission needs documented in the revised Mission Needs Statement.

Question. How much does the Coast Guard estimate the cost of a covert surveillance aircraft to be?

Answer. The rough order of magnitude acquisition cost of a fully missionized, FAA-certified manned covert surveillance aircraft is estimated to be $8 million.

Question. What is the timeline for acquiring a covert surveillance aircraft or aircrafts for operational use?

Answer. The procurement timeline is currently being constructed with the Manned Covert Surveillance Aircraft acquisition team. The following table provides the best estimate of initial operating capability (IOC).

Operational Requirements Document Written & Approved	July 2005
Release of Request for Proposal	September 2005
Aircraft Award	January 2006
Airworthiness Certification Test/Evaluation Commencement	January 2007
Initial Operating Capability	January 2006

Question. Are there existing platforms available on the commercial market that would meet the Coast Guard's specifications for a covert surveillance aircraft? If so, please describe them.

Answer. Currently, the Coast Guard is developing the operational requirements and specifications for the Manned Covert Surveillance Aircraft. Once these are defined and approved, the Coast Guard will conduct a formal market survey and or request for proposal to determine the availability of any suitable aircraft in the commercial market that meets its requirements.

AUTOMATIC IDENTIFICATION SYSTEM

Question. The Coast Guard has obligated $7.5 million to a contract with a commercial low earth orbit satellite communications provider for the installation of AIS capability on a concept validation satellite and design for installation on future satellites. What type of coverage does this provide to the Coast Guard?

Answer. The deployment of a concept validation payload aboard a commercial low earth orbit satellite is a prototype for the receipt of AIS signals via satellites from vessels within 2000 nautical miles of the U.S. coast.

Question. The AIS budget provides for approximately $30 million per year over the next five fiscal years (including fiscal year 2006). Could this acquisition program be accelerated if additional funding became available?

Answer. The Coast Guard's fiscal year 2006–2010 Capital Investment Plan calls for project completion in 2011; however, the project could be completed sooner if additional funding is provided.

COAST GUARD SUPPORT OF NSF RESEARCH OPERATIONS IN THE POLAR REGIONS

Question. The budget request for the National Science Foundation includes $48 million in budget authority to operate and maintain the 399 foot Polar Icebreakers. This amount does not include funding such as extraordinary maintenance costs. In fiscal year 2005, these extraordinary maintenance costs are estimated to be $18 million. The budget indicates that a Memorandum of Understanding (MOU) is being discussed to address these additional costs. What is the status of the MOU between the National Science Foundation (NSF) and the U.S. Coast Guard?

Answer. The Coast Guard and NSF are currently negotiating to conclude an MOU for fiscal year 2006.

The $48 million NSF budget authority represents the base funding to operate and maintain the 399 foot POLAR STAR and POLAR SEA and the 420 foot HEALY. The MOU will reflect an agreement between NSF and Coast Guard for NSF to pay for all personnel, maintenance and operational funds necessary to manage the polar icebreaking program.

The Administration plans to maintain current polar icebreaker fleet capabilities at least until a new national polar icebreaker requirements policy decision is made.

Question. Please provide a historical breakdown, by fiscal year, of the costs to support the NSF's scientific and operational programs in the Polar Regions, including maintenance costs, and how much the NSF reimbursed for those costs in each fiscal year.

Answer. In recent years, the Coast Guard icebreaker fleet has devoted, on average, 82 percent of its operational time in support of the NSF. The chart below attributes NSF's percentage of operational time to the total annual funding for the icebreakers (including maintenance costs).

The following table provides a historical breakout of Coast Guard polar icebreaking support costs, those costs attributable to NSF activities, and the amounts reimbursed by NSF to the Coast Guard per the MOA between the two agencies.

Fiscal year	Reimbursement Amount from NSF	Total Costs required to support cutters [1]	Percent Operational time devoted to NSF	Cost to support NSF programs
1999	$2,711,732	$31,397,056	76	$24,004,075
2000 [2]	2,145,242	40,971,438	80	32,777,150
2001	4,966,672	41,899,046	64	26,839,661
2002	5,961,684	49,195,000	93	45,643,381
2003	8,165,647	50,501,309	91	45,925531
2004	12,422,190	57,585,544	89	51,189,137

[1] Note: Costs include actual unit level operating and maintenance costs, fuel costs, depot level maintenance costs, and personnel costs for the salaries and benefits attributable to the people assigned to the cutters. These costs have grown to exceed budgeted amounts due to extraordinary maintenance costs required to sustain the polar icebreaking fleet. The President's fiscal year 2006 budget proposes transfer of the Coast Guard's base funding (using budgeted amounts) to support operation and maintenance of these cutters.

[2] Reflects the addition of the HEALY as the third Coast Guard icebreaker.

Question. If a Memorandum of Understanding is not reached and the NSF decides to contract out for their icebreaking needs in the polar region, would the Coast Guard need to maintain the Polar Sea and the Polar Star icebreakers?

Answer. On August 8, 2005, the Coast Guard signed an MOU with NSF to ensure that the polar icebreaking fleet will be operated and maintained in fiscal year 2006.

Question. If so, what functions would they serve and what would be the costs in fiscal year 2006?

Answer. The polar class icebreakers (POLAR SEA and POLAR STAR) have been and will continue to primarily support the U.S. Antarctic Program re-supply effort (Operation Deep Freeze) each year. Due to Antarctic ice conditions, the age of the vessels and the breakers' increasing maintenance needs since 2001, these two vessels are no longer able to support simultaneously the U.S. Antarctic Program. Pending additional funding from the NSF in fiscal year 2006, POLAR SEA will continue the second year of a 2-year maintenance availability to ensure readiness for the Operation Deep Freeze 2007 deployment to Antarctica. POLAR STAR is currently scheduled to support the 2006 Operation Deep Freeze mission. HEALY is scheduled to support Arctic research, typically lasting from May to November of each year. The fiscal year 2006 base funding and overall costs are outlined below:

FISCAL YEAR 2006 COAST GUARD POLAR ICEBREAKER BASE FUNDING

Projected costs AFC	Cost center HEALY	POLAR SEA	Fiscal year 2006 POLAR STAR	Total
Training & Recruiting	$210,512	$355,244	$355,244	$921,000
Military Personnel	5,936,630	9,547,685	9,547,685	25,032,000
Depot Level Maintenance	4,498,926	4,493,037	4,493,037	13,485,000
Operating and Maintenance	3,586,000	2,000,000	2,000,000	7,586,000
Central Accounts	109,000	183,500	183,500	476,000
Grand Total	14,341,068	16,579,466	16,579,466	47,500,000

FISCAL YEAR 2006 PROJECTED COSTS REQUIRED TO SUSTAIN POLAR ICEBREAKER FLEET ABOVE THE BASE FUNDING LEVEL

Projected costs AFC	Cost center HEALY	POLAR SEA	Fiscal year 2006 POLAR STAR	Total
Depot Level Maintenance	$7,100,000	$9,700,000	$500,000	$17,300,000

Question. If not, what would be the cost for the Coast Guard to mothball or dispose of the two icebreakers?

Answer. The Coast Guard estimates that the cost to mothball or dispose of each Polar Class Icebreaker is $750,000 per hull, for a total of $1.5 million.

The estimated personnel transfer cost if the two icebreakers are decommissioned is $700,000.

Question. What are the long-term costs to maintain the Coast Guard's Polar Icebreakers?

Answer. The two heavy polar icebreakers are nearing the end of their service lives and require major systems overhauls to continue to operate in a cost-effective manner. The Coast Guard has not developed detailed analyses of the costs associated with the long-term costs of recapitalizing the heavy polar icebreaking fleet. As the national needs for heavy polar icebreaking are more thoroughly studied by the National Academies of Sciences (NAS), the Coast Guard will inevitably be involved in developing long-term cost estimates for heavy polar icebreaking.

Since the Healy medium-duty polar icebreaker is a relatively new vessel, there are no significant long-term maintenance costs above the budgeted base amounts for that ship.

Question. What efforts are underway to fund a replacement vessel or overhaul one or more of the existing vessels to support the long-term needs of the scientific community?

Answer. There are no plans to replace or overhaul CGC HEALY, which was commissioned in 2000.

In accordance with the fiscal year 2005 Homeland Security Appropriations Bill Conference Report, the NAS will be conducting a polar icebreaker study, with an interim report expected during November 2005 and completion of the final report anticipated during July 2006. The NAS study report could be used as the basis for an update of the 1990 Presidential Decision Determination on national polar icebreaker requirements policy.

Question. What would the cost be and the amount of time necessary to acquire a new polar icebreaker?

Answer. Initial rough estimates indicate that one new polar icebreaker, with the equivalent heavy icebreaking capabilities as the Polar Class icebreakers, would cost approximately $600 million and would require 6 years to construct.

Question. The Coast Guard is absorbing roughly $9 million in fiscal year 2005 to meet key milestones in the maintenance of the Polar Sea. Is critical maintenance in other areas being delayed or canceled to meet the needs of the Polar Sea?

Answer. Yes, the $9.2 million for extraordinary maintenance of the POLAR SEA will be absorbed within the Coast Guard's fiscal year 2005 maintenance funds, requiring deferral of critical maintenance in other areas, such as replacement of aging and obsolete subsystems onboard Coast Guard legacy cutters.

Question. If so, please describe those delays and the impact they will have on the Coast Guard fleet.

Answer. As the end of fiscal year 2005 approaches, and the level of fleet-wide unscheduled maintenance activity becomes clearer, specific maintenance activities will

be identified for deferral by Coast Guard maintenance managers as they shift resources to deal with their most immediate fleet maintenance challenges.

Question. Section 888 of Public Law 107–296 ensures that Coast Guard "functions and capabilities be maintained intact and without significant reduction." Under what authority does the proposal to transfer funding for icebreaking operations to the NSF fall under?

Answer. Subsection 888(c) of the Homeland Security Act of 2002 provided that: "the authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction after the transfer of the Coast Guard to the Department, except as specified in subsequent Acts."

The proposed shift of appropriations for polar icebreaking, if enacted, does not remove any of the authorities, functions, or capabilities of the Coast Guard. Since NSF and the Coast Guard have a signed MOU ensuring funding for the icebreaking program in fiscal year 2006, the Coast Guard will continue to perform its polar icebreaking mission. Furthermore, the proposed shift of appropriations, if enacted, would be the result of a "subsequent act" of Congress, in the terms of Subsection 888(c).

RECRUITING

Question. What is the Coast Guard's goal for recruiting active duty personnel in fiscal year 2006? Provide a chart showing the total number of recruits in each of the past 10 years for active duty personnel and reserves and compare them against the Coast Guard's targets for those years.

Answer. The following tables show the total number of Coast Guard active duty and reserve recruits in each of the past 10 years compared with the Coast Guard's targets for those years.

COAST GUARD ACTIVE DUTY RECRUITING

Year	Targets	Accessed
1996	3,300	3,299
1997	3,900	3,697
1998	4,464	3,962
1999	4,150	4,159
2000	4,700	4,721
2001	4,300	4,332
2002	4,800	5,169
2003	4,475	4,488
2004	3,800	3,809
2005	4,110	[1] 4,110
2006	[1] 4,200	[1] 4,200

[1] Projected.

COAST GUARD RESERVE RECRUITING

Year	Targets	Accessed
1996	350	229
1997	430	303
1998	1,313	554
1999	900	801
2000	900	692
2001	700	424
2002	718	585
2003	1,150	880
2004	940	911
2005	950	[1] 800
2006	[1] 900	[1] 900

[1] Projected.

C–130JS

Question. In March, the Coast Guard placed interim limitations on the HC–130H 1500 series aircraft. What is the status of these restrictions?

Answer. The HC–130H 1500 series aircraft are operationally restricted/limited based on potential cracking in the center wing box based on effective wing age. The

restrictions on the five Coast Guard 1500 series aircraft are similar to restrictions imposed on United States Air Force aircraft of similar vintage and use rate. The restrictions are designed to limit wing loading by limiting fuel, cargo and airspeed under certain conditions. These restrictions will remain in place until Lockheed Martin Aero (LMA) Service Bulletin (SB2) is developed and the required inspections are completed. SB2 is expected on May 30. Each aircraft inspection will take approximately 1 month to complete. If serious structural cracking is found during inspections, the Coast Guard will determine whether to refurbish the affected aircraft to keep them in service well into the future or if there are other alternatives.

Question. What impact have these restrictions had on the Coast Guard?

Answer. The restrictions currently impact only the five 1500-series C–130s at Coast Guard Air Station Elizabeth City and have resulted in some degradation of the unit's ability to perform long-range search and rescue, maritime patrol, logistics and International Ice Patrol missions. These operational restrictions are based on reduced fuel and cargo loads similar to those imposed on United States Air Force aircraft of similar vintage and use rate. The restrictions reduce the maximum endurance of the aircraft from 12 to 7.5 hours, reduce the maximum cargo capacity from 45,000 to 10,000 lbs, require slower airspeed when in the vicinity of turbulence and require greater fuel reserves. These restrictions have been mitigated by incorporating more refueling stops and or using newer 1700-model C–130s without restrictions.

Question. What are the Coast Guard's plans to remedy the structural problems, including necessary funding?

Answer. There are no known structural problems to be remedied. The 1500 series aircraft are operationally restricted/limited based on the potential of cracks in the center wing box based on effective wing age. LMA is currently developing the procedures to inspect the wings to determine if cracks exist. If inspections find no evidence of structural cracking, the operational restrictions will be adjusted or removed. If serious structural cracking is found during inspections, the Coast Guard will determine whether to refurbish the affected aircraft to keep them in service or if there are other alternatives. Cost estimates to effect necessary repairs will be based on the results of the inspections.

SIPRINET

Question. The Coast Guard is in the process of increasing its SIPRNET presence to include all of its major shore side operational units (Areas, Districts, Sectors, & Air Stations). Approximately half of the planned shore side Coast Guard units (80 out of 156) currently have SIPRNET connectivity. What is the funding level for this activity in fiscal year 2006?

Answer. The Coast Guard SIPRNET Program is fiscal year 2006 base of funds is $9.5 million. This includes funding for recurring circuit costs, contract labor costs, new installations, and equipment recapitalization.

Question. What is the current schedule to provide connectivity to the remaining units?

Answer. The Coast Guard is currently planning to fund the installation of 23 new sites during fiscal year 2006. The Coast Guard anticipates completing SIPRNET installations at all 152 sites by fiscal year 2009.

Question. Could the schedule be accelerated if additional funding became available in fiscal year 2006?

Answer. Additional funding in fiscal year 2006 would not accelerate the installation schedule. The installations are currently scheduled at maximum install rate due to the time required to build the facilities and installation contractor resource capabilities.

MARITIME SECURITY CUTTER—LARGE OPERATIONAL COSTS

Question. The Coast Guard is expecting the first WMSL to be delivered in May 2007. Please provide a spend plan and timeline related to the funding necessary for pre-commissioning familiarization and training for core personnel.

Answer. The timeline for pre-commissioning training and familiarization is as follows:

—*Phase I: Winter/Spring 2005.*—Five crewmembers reported to Pascagoula for pre-arrival training, ship engineering familiarization, and doctrine development. Cost: $151,352

—*Phase II: Summer/Fall 2006.*—96 crewmembers report to Alameda (the ship's homeport) to conduct pre-arrival training, which is provided at various government and commercial facilities around the country. Following pre-arrival train-

ing, these crewmembers will proceed to Pascagoula for pre-commissioning familiarization. Cost: $1,830,816

—*Phase III: Winter/Spring 2007.*—Remaining 61 crewmembers report to Alameda then immediately proceed to Pascagoula for pre-commissioning familiarization. Cost: $1,063,930

—*May 2007.*—First National Security Cutter/Maritime Security Cutter Large (WMSL) is delivered to the Coast Guard.

The travel and subsistence cost for crewmembers to complete the initial pre-arrival and pre-commissioning training is estimated at $3.1 million.

RESEARCH & DEVELOPMENT

Question. Section 888 of Public Law 107–296 ensures that Coast Guard "functions and capabilities be maintained intact and without significant reduction." Under what authority does the proposal to shift Cost Guard R&D functions to the S&T Directorate fall under?

Answer. Subsection 888(c) of the Homeland Security Act of 2002 provided that: "the authorities, functions, and capabilities of the Coast Guard to perform its missions shall be maintained intact and without significant reduction after the transfer of the Coast Guard to the Department, except as specified in subsequent Acts."

The proposed shift of appropriations for Research, Development, Test and Evaluation from the Coast Guard to the S&T directorate, if enacted, would be the result of a "subsequent Act" of Congress, in the terms of Subsection 888(c).

Question. How would the proposed transfer improve the ability of the Coast Guard to accomplish its missions?

Answer. The consolidation of Research and Development (R&D) funding at the Department level will maximize effectiveness of R&D activities across the Department by minimizing redundancies. Through the Coast Guard portfolio manager at S&T, the Coast Guard will continue to develop and provide homeland and non-homeland security research requirements which support all of the Coast Guard's homeland and non-homeland mission programs.

ATTRITION RATE

Question. What is the current attrition rate for Secret Service agents and Uniformed Division Officers?

Answer. In fiscal year 2004, the attrition rate for special agents was 6.28 percent, and for Uniformed Division officers 7.6 percent. The Secret Service expects that the attrition rate for fiscal year 2005 for special agents will be 5.2 percent, and for Uniformed Division officers 8.5 percent.

OVERTIME RATE

Question. What is the current monthly overtime rate for Secret Service agents?

Answer. The current average monthly overtime rate for Secret Service agents is 71 hours.

PAY INCREASE

Question. The budget includes funding for a 2.6 percent pay increase for Secret Service employees in 2006, but the Administration requested a 2.1 percent across the board pay increase for Federal employees. Why is the Secret Service budgeting for a higher pay increase?

Answer. The Secret Service's fiscal year 2006 budget includes funding for a 2.3 percent pay increase for Federal employees. This is the same percentage increase proposed by the Administration.

Question. What is the cost difference between a 2.1 percent pay increase and a 2.6 percent pay increase?

Answer. A 2.1 percent pay increase would require $11,752,000, and a 2.6 percent pay increase would require $14,550,000, a difference of $2,798,000. The Secret Service request was $12,871,000 or 2.3 percent.

WHITE HOUSE MAIL

Question. The budget includes $16.365 million to process White House mail. What is the status of the Department's efforts to develop a long-term plan for a fully operational White House Mail facility?

Answer. In the summer of 2004, the U.S. Secret Service and the General Services Administration (GSA) initiated the planning of a permanent White House mail facility.

The stakeholders utilized two previous studies in order to begin their effort. In 2003, the Secret Service commissioned Science Applications International Corporation (SAIC) to develop a full-scale mail screening facility in concept. In addition, GSA conducted a site selection study in which they identified four feasible locations in the Washington, D.C. metropolitan area for a White House mail facility.

In October 2004, GSA procured the services of HDR, an architectural engineering and consulting firm, to complete a Program Development Study (PDS). The PDS, which was completed in February 2005, reflects the efforts of the team to define the feasibility, analyze needs, prepare cost analysis and program requirements for the program. A mail screening facility proposal was defined by the PDS. Three sites located at the Anacostia Naval Annex were selected as most feasible. The PDS estimated the cost for construction at $33.5 million.

Since the completion of the PDS, the development team has worked closely with GSA to identify a potential future site for the White House mail screening facility. GSA is working with the Navy Real Estate Office to assess the availability of property at the Anacostia Naval Annex, in Washington, D.C. adjacent to other White House support facilities for this purpose. Upon identification of available Federal property, GSA will conduct environmental and design studies of the potential site. This information will be used to determine the GSA facility acquisition plan (lease/build) and project the new facility's operational costs.

Question. What is the percentage of mail addressed to the White House that doesn't reach its destination?

Answer. For the 14-month period beginning in March 2004 and ending April 2005, the White House mail screening facility received approximately 1,730,000 pieces of mail, flats or parcels. Of these, 288,800 items (or 16 percent) were classified as junk mail and, therefore, not processed at the facility. Of the remaining 1,441,200 processed mail pieces, 1,441,000 (or 99.9 percent) pieces were delivered to the complex.

The two hundred pieces of mail (or less than 1 percent) not delivered to the complex were identified by the facility as containing an unknown substance or an overt threat and were referred to the Secret Service Intelligence Division for investigation. In addition, 29 referrals were made to Secret Service field offices due to items received at the facility and two arrests were made.

EMERGENCY RESPONSE FUND

Question. The latest report (date) from OMB on the status of the $40 billion Emergency Response Fund, enacted 3 days after 9/11, shows that the Secret Service has an unobligated balance of $6 million. Why have the funds not been used and what are your plans for the unobligated funds?

Answer. As of October 2004, the Secret Service had no unobligated balance from the Emergency Response Fund.

NATIONAL RESPONSE PLANNING

Question. DHS has recently released the National Incident Management System Plan, the Nation Preparedness Goal and begun the roll out of the National Response Plan which will better guide the spending of Federal resources like the over $11 billion Congress has appropriated for first responders programs. With this additional guidance, what changes have you seen/do you expect to see in the local requests for projects that will prevent wasteful spending?

Answer. The National Incident Management System (NIMS) integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. The NIMS will enable responders at all levels to work together more effectively to manage domestic incidents no matter what the cause, size or complexity. The Department is requiring that states and territories begin work on compliance with the NIMS as part of their fiscal year 2005 grant funding.

The National Response Plan (NRP) establishes a comprehensive all-hazards approach to enhance the ability of the United States to manage domestic incidents. The plan incorporates best practices and procedures from incident management disciplines—homeland security, emergency management, law enforcement, firefighting, public works, public health, responder and recovery worker health and safety, emergency medical services, and the private sector—and integrates them into a unified structure. It forms the basis of how the Federal Government coordinates with State, local, and tribal governments and the private sector during incidents.

The National Preparedness Guidance, issued on April 27, 2005, addresses the implementation of the NIMS and the NRP, as one of the overarching national priorities. DHS is now beginning to work with states, territories, and urban areas to update their existing State and urban area homeland security strategies to bring them

into alignment with the seven national priorities. This alignment with the national priorities will enable States and territories to continue expending funds in accordance with the goals and objectives already outlined in the strategies. With this, DHS expects a greater emphasis on training and exercises to further implement the NRP and NIMS within the States and territories. Historically, there has been a higher trend towards the purchase of specialized equipment, but DHS believes that the States are undertaking training and exercise programs that typically require longer-term planning.

Question. How have the State and local entities reacted to the changes?

Answer. State and local entities have had many questions about the publication of all three of these documents. Understandably, they do not always clearly understand the intent of the documents and how they are related to the grant funding that they receive. Likewise, they are concerned about the resources they will need at the State level to ensure compliance. Anticipating such concerns, DHS created on-line training materials through FEMA/USFA's Emergency Management Institute and National Fire Academy's Distance Learning Programs that cover both NIMS and the NRP. To date, more than 200,000 personnel have completed these training courses. In order to further articulate these requirements, the Department has scheduled several rollout conferences for the NIMS and NRP across the country to educate the State and local stakeholders. The NIMS Integration Center (NIC) is responsible for orchestrating NIMS implementation and NIMS compliance. Through training, exercises, and technical assistance, the NIC is working to ensure that our state, local, and tribal partners understand NIMS and take the appropriate steps to implement it in their communities. In addition to the NIMS and NRP outreach, the Office for Domestic Preparedness (ODP), within SLGCP, has scheduled three additional meetings on the National Preparedness Guidance so that States and territories understand the imbedded requirements. We also are offering technical assistance packages that are customized to each State and territory. ODP is committed to providing additional education and outreach to our grantees as we move forward in implementing the seven national priorities codified in the National Preparedness Guidance.

SLOW PACE OF GRANT DISTRIBUTIONS

Question. On October 18, 2004, the President signed into law the fiscal year 2005 Homeland Security Appropriations Act. The majority of the grants funds have just recently been made available for application this month: 6 months since the Act was signed into law. Rail security funds were made available on April 5, 2005. Transit security funds were also just made available on April 5, 2005. Port security funds, as of April 20, 2005, still have not been made available for application. The State Homeland Security Grant Program is the only program that has awarded funding and that is because the Congress required it by law. None of the other fiscal year 2005 homeland security grant funds have actually been distributed.

Why is it taking so long to get the money out the door?

Answer. The responsibility for most non-aviation grant programs was transferred from the TSA to SLGCP during fiscal year 2004. This resulted in a transition period while programs and staff adapted to different processes and new automation. More importantly, the Department has used this time to work with Federal partnering agencies and applicable state, local, and private sector stakeholders to redesign these programs to include a more risk-based approach to allocation of funding that aligns with Administration priorities as described in Homeland Security Presidential Directive (HSPD)-8 and the recently released National Preparedness Goal. The Department is committed to awarding grants earlier in the year while maintaining effective oversight.

Question. What steps are being taken to expedite the process?

Answer. Completion of the programmatic redesign process coupled with automation of the application submission, reporting, and payment processes for these programs will result in greatly enhanced processing capabilities for future program funding. In addition, SLGCP has established the Transportation Infrastructure Security Division to manage these programs. The Division is in the process of filling remaining vacancies and consequently will be in a greatly strengthened position for management and administration of future grant programs.

Question. When will funding be awarded for Intercity Passenger Rail Security, Transit Security, Intercity Bus Security and Port Security grants?

Answer. The current schedule for each program is as follows: Intercity Passenger Rail Security Program—awarded July 18, 2005; Transit Security Grant Program—awarded July 15, 2005; Intercity Bus Security Grant Program—first round of awards were awarded on August 9, 2005, and the final round of awards will be

awarded on September 30, 2005; Port Security Grant Program—awarded September 1, 2005.

Question. As part of your Department review, will you commit to expediting the grant making process so that money that is supposed to make Americans safer does not sit in the Treasury in Washington, DC?

Answer. The Department takes its responsibility very seriously for protecting Americans and the critical transportation infrastructure they depend on. As stated previously, the recent redesign of these programs, coupled with the newly instituted SLGCP Transportation Infrastructure Security Division and automation of the application, reporting, and payment processes for these programs will result in significantly enhanced capabilities relative to the management and administration of these programs. In addition, SLGCP is also in the process of establishing an Office of Grants Operations that will further streamline financial management activities associated with these grants.

PORT/RAIL/TRANSIT

Question. According to the American Public Transportation Association, there are approximately 9.6 billion transit trips annually and people use public transportation vehicles over 32 billion times each workday. This is more than 16 times the number of aviation passengers, and yet the Department continues to spend less than 10 percent of its transportation security resources on non-aviation security. The President's Budget Request proposes that individual grant programs for port, rail/mass transit, bus, and truck security grant programs be eliminated and collapsed into a new grant program called a "Targeted Infrastructure Protection Grants" program. Because none of the previous individually appropriated grant programs are specified in this new account—ports will compete against rail and mass transit, and other infrastructure for $600 million. For mass transit security alone, the American Public Transportation Association estimates a need for $6 billion in transit security. Not only does this insufficient request show a lack of support for modes of transportation other than air travel security but it further frustrates the officials responsible for securing people's safety on these modes by pitting them against each other for scarce resources. We currently spend $5 billion on aviation security. This proposal continues a disturbing pattern by the Department of focusing on the last battle—aviation security—and less on non-aviation modes of transportation.

How does the agency really expect that this request furthers the mission of homeland security when we are only as strong as our weakest link?

Answer. Enhancing the security of the Nation's critical infrastructure, including transportation, continues to be a high priority for the Department, which is why the Department proposed the development of a Targeted Infrastructure Protection (TIP) Program. This program would consolidate Port Security, Rail/Transit Security, Intercity Bus Security, and Trucking Industry Security grant programs into a single larger program. Because it is unrealistic to anticipate infrastructure threats and protection needs nearly 12 months in advance, the Secretary requires flexibility to target valuable TIP resources to address emerging needs, risks, and national priorities. Moreover, funds for this program will also allow the Department to build on and leverage partnerships with other Federal agencies and industry that seek to advance the State of the Nation's preparedness through better security solutions and information sharing approaches. Because the program is designed to provide us with maximum flexibility at the appropriate time, the Department is confident that the TIP will help further the mission of securing the homeland. The Administration requested a nearly 50 percent increase in total infrastructure funding in order to reduce concerns about "competition" among various sectors.

ALL-HAZARDS

Question. The fine men and women of FEMA have recently responded to wildfires in Alaska, mudslides in California, and hurricanes in Florida in an unprecedented period of activity. As the backbone of the nation's all-hazards emergency management system the Emergency Management Performance Grants (EMPG) Program, now administered by the Office of State and Local Government Coordination and Preparedness, is the only direct source of Federal funding to assist State and local governments with planning and preparedness activities associated with natural disasters. Congress saw fit last year to reject the President's proposal to cap allowable salary expenses and to shift the program away from its all-hazards philosophy. Secretary Chertoff said on March 2 of this year "while fighting terrorism was the reason for the department's creation, it is not our sole function," which implies that all-hazards prevention, preparedness, response and recovery is a priority of DHS.

Yet, a proposed $10 million cut in the EMPG program appeared in the Budget Request.

Why is it that the President proposes a $10 million cut in this program?

Answer. The Department's fiscal year 2006 Budget request of $170 million for the Emergency Management Performance Grants (EMPG) Program remains consistent with the fiscal year 2005 request and demonstrates a continued strong commitment and support to the nation's emergency prevention and response community through an all-hazards approach. In fiscal year 2006, EMPG will provide support for State and local emergency management departments and agencies based on identified needs and priorities for strengthening their emergency management capabilities, while addressing homeland security concerns. Further, the integration of EMPG into the Homeland Security Grant Program umbrella results in synergies with other related homeland security assistance programs. In addition, this integration also has facilitated efforts by states/local jurisdictions to leverage homeland security assistance to accomplish goals and objectives in their homeland security strategies.

FIRE GRANT FUNDING

Question. Each day firefighters put themselves in harm's way to protect property and help citizens in time of need. There are currently over 1 million active firefighters in the United States, and about 73 percent of those volunteer. According to the U.S. Fire Service, many fire departments report shortfalls in facilities, equipment, and training of personnel particularly volunteer companies in rural communities. An estimated one-third of firefighters per shift are not equipped with self-contained breathing apparatus. In communities under 10,000 in population that have at least one building 4 stories high or higher, 10 percent are estimated to have no ladder or aerial apparatus. The assessment also found that overall fire departments can only equip about half of the emergency responders on a shift with portable radios. Additionally, 21 percent of fire departments, nearly all of them predominately volunteer departments, have four or fewer firefighters available in a mid-day fire house which means it is likely that the departments fail to deliver the minimum of 4 firefighters needed to safely initiate an interior attack on a fire. Fiscally stressed communities make every effort to support public servants but State and local funding simply is not there. Yet, the President proposes to reduce firefighter grants from $715 million to $500 million. In addition, he proposes to eliminate funding for the SAFER program, which Congress authorized to help communities hire firefighters.

Please explain how the President's proposed 30 percent cut in funding helps fill these gaps.

Answer. The Department's fiscal year 2006 Budget request reflects a strong commitment to our nation's fire service by providing $500 million for the Assistance to Firefighters Grant Program. This request is consistent with the Administration's budget request since fiscal year 2003 and reflects the appropriate balance of funding priorities among DHS grant programs. Further, this program has been in existence for 5 years and has 4 years of grant experience. In its reauthorization, Congress directed that an update to an assessment of the needs of the fire service be done, as the prior assessment does not reflect the impact of more than $2 billion in grant funding that DHS has provided to the nation's fire service over the last 3 years, both through Assistance to Firefighter Grants and Homeland Security Grants. In fact, the nation's fire service has received more DHS grant funding than any other public safety discipline. This report is expected to be completed in February or March 2006. In addition, Firefighting Operations and Support for terrorist attacks, major disasters, and other emergencies is among the national target capabilities identified in the forthcoming National Preparedness Goal. Finally, it is important to note that there is significant funding available for similar purposes included in other programs, such as the State Homeland Security Program and the Urban Areas Security Initiative.

Question. Also, please explain why the President proposes to terminate the SAFER firefighter hiring program.

Answer. The Administration has requested significant funds over several years to support public safety preparedness at the State and local levels of government. Over the last 3 years, Congress has appropriated and DHS has granted over $12 billion to support training, exercising, and equipping public safety personnel, including firefighters, across the nation. The Administration maintains that hiring firefighters should remain a local responsibility, as local resources will eventually be needed to retain newly hired personnel. To that end, Federal support should focus on enhancing local capacities through training, equipment, and exercises; and not building inherently local capacities.

INTEROPERABILITY COMMUNICATIONS

Question. Over $800 million in grant funding has been distributed for interoperability projects. The next largest specific first responder category—at less than half of that—is regional response teams funding. The Intelligence Reform Act authorizes a new DHS grant program for interoperability as well as a pilot program and the ability to establish and Office of Interoperability and Compatibility.

What lessons learned or best practices has the agency gleaned from the fiscal year 2003 demonstration with COPS and FEMA?

Answer. The "fiscal year 2003 demonstration" refers to the competitive grant program that COPS, FEMA, and SAFECOM collaborated on to maximize the funding available for interoperable communications equipment. The program provided competitive funding to local jurisdictions to demonstrate effective solutions for achieving interoperability. The lessons learned from this program have been incorporated into SAFECOM's coordinated grant guidance.

SAFECOM, a program of the S&T Directorate's Office for Interoperability and Compatibility (OIC), is the umbrella program within the Federal Government that oversees all initiatives and projects pertaining to public safety communications and interoperability. SAFECOM's coordinated grant guidance provides the public safety community with consistent guidance, coordinated application processes, similar requirements across grant programs, and general guidelines for implementing a successful wireless communications system. This guidance seeks to incorporate best practices and lessons learned from the fiscal year 2003 demonstration program. The guidance was incorporated in the fiscal year 2003 FEMA and fiscal year 2003/fiscal year 2004 COPS grant awards, as well as ODP grant packages in fiscal year 2004. Examples of the lessons learned which are incorporated into the grant guidance include:

—General criteria relating to public safety communications grants;
—Criteria specific to block grants allocated to states;
—Additional criteria based on the lifecycle of public safety communications projects;
—Additional guidelines, examples, and resources for improving public safety communications and interoperability, and implementing a wireless communication system; and
—A thorough list of questions that applicants can use to help ensure that they have taken into account the needs of public safety, potential partners, and considered short and long-term goals.

SAFECOM's coordinated grant guidance is available at www.safecomprogram.gov.

Question. Outside of equipment acquisition what are the obstacles to interoperability?

Answer. While equipment acquisition is a substantial obstacle, there are many other significant challenges to achieving interoperability. In a February 2003 report, the National Task Force on Interoperability identified five key challenges facing the development of interoperability, including: limited and fragmented radio spectrum, lack of coordination and cooperation, limited and fragmented funding, incompatible and aging communications equipment, and limited and fragmented planning.

DHS understands the complexity of the problem of interoperability. The OIC, through SAFECOM—the umbrella program within the Federal Government that oversees all initiatives and projects pertaining to public safety communications and interoperability—has developed the Interoperability Continuum to serve as a framework for addressing the obstacles to interoperability, beyond just equipment. The Continuum helps the public safety community and local, tribal, state, and Federal policy makers address critical elements for success as they plan and implement interoperability solutions. These elements include governance, standard operating procedures, technology, training/exercises, and usage of interoperable communications. Making progress in each of the five critical elements is crucial to the Department providing guidance to overcome the obstacles to interoperability.

INTEROPERABILITY STANDARDS

Question. What is the status of national standards for interoperable communication?

Answer. DHS has made significant strides in the development of national standards and requirements for interoperable communications through SAFECOM. SAFECOM has developed accelerated standards for public safety interoperable communications, and drafted a report as required by IRTPA that discusses DHS plans for accelerating standards. This report includes a schedule of milestones and achievements. The report is moving through the clearance process and will be sent to Congress immediately therafter.

DHS recognizes that the development of standards can only occur within the context of an architectural framework. The SAFECOM process for identifying and developing standards begins with development of a practitioner-accepted statement of requirements which then drives the development of a Public Safety Architecture Framework (PSAF). SAFECOM released Version 1.0 of the first comprehensive Public Safety Communications and Interoperability Statement of Requirements (SoR) in 2004. Developed with public safety practitioner input, the SoR defines the functional requirements for public safety practitioners to communicate and share information when it is needed, where it is needed, and when authorized. SAFECOM, in cooperation with the National Institute of Standards Technology's (NIST) Office of Law Enforcement Standards (OLES), completed a draft of the PSAF, currently being reviewed for publication. The architectural framework outlines what the overall structured approach is for facilitating interoperability and indicates how the architecture will operate through the development of interface standards.

Since the release of v1.0 of the Public Safety Communications and Interoperability SoR, SAFECOM has undertaken the development of v1.1 of the SoR. SoR v1.1 will reorganize the requirements contained within v1.0 into a layered structure, reclassifying the requirements into Network Functional Requirements, Device Functional Requirements, and Application/Services Functional Requirements. SAFECOM is currently vetting v1.1 of the SoR with the public safety practitioner community and anticipates releasing v1.1 to the public upon completion of that vetting process.

Development of v2.0 of the SoR is currently underway. SoR v2.0 will add additional quantitative values to the functional requirements contained in v1.1, as well as address NIMS compliance. SAFECOM anticipates that it will be able to vet the draft of this version with the public safety community beginning in early 2006.

Question. What other equipment does DHS plan to publish standards for and when will those standards be published?

Answer. The Standards Portfolio in the S&T Directorate is working with voluntary consensus standards organizations and the National Institute of Standards and Technology (NIST) to develop standards in many areas of homeland security. In the CBRNE area, standards should be published in fiscal year 2005-fiscal year 2006 for: radiation detection (portal monitors, neutron detectors, training and data format); suspicious powder protocols, trace explosive detection; and chemical agent vapor detection. Standards for CBRNE personal protective equipment for emergency responders are being developed for: powered air purifying and self contained breathing respirators; chemical/biological hot and warm zone ensembles; personal alert safety systems; thermal exposure measurement; law enforcement PPE; and a bomb suit. Standards are also in development for biometric evaluation protocols, user interface guidelines, image quality. Standards efforts are in progress for: building security personal identity verification and access control; gaseous air cleaning; economic standards for security-related issues; and design/economics for structural integrity. Check lists for security of information technology products and PDA forensic tools have been published. Finally, SAFECOM is working with NIST's OLES and other Federal partners to accelerate the publishing of relevant radio standards for public safety interoperable communications in fiscal year 2006-fiscal year 2007. Standards for the Inter-Sub-System-Interface, Console Interface, and Fixed Station Interface will pave the way for future seamless communications. Standards for basic functionality will be published by the second quarter of fiscal year 2006, with the balance of the functions being published by the second quarter of fiscal year 2007.

NON-PROFIT GRANT FUNDING

Question. In fiscal year 2005, $25 million was provided for non-profits for security at high-threat facilities. Who have these awards been distributed to, for how much and for what purpose?

Answer. The $25 million was provided to protect nonprofit organizations located in the top 18 urban areas receiving funds in the fiscal year 2005 UASI program. These funds are to be used for target hardening, which includes the acquisition and installation of security equipment in real property (including buildings and improvements) owned or leased by a nonprofit organization, specifically in response to a risk of terrorist attack. Specific allocations for urban areas are available in the fiscal year 2005 Homeland Security Grant Program (HSGP) program guidelines and application kit, which can be found at the following website address: http://www.ojp.usdoj.gov/fundopps.htm

Question. Do funds remain available for obligation? If so, how much?

Answer. Upon receipt of fiscal year 2005 funds awarded through the HSGP, States were required to issue a solicitation within 60 days of the award date for or-

ganizations to apply for funds allocated for nonprofit organizations. States are currently in the process of finalizing these awards.

EMS FIRST RESPONDER FUNDING

Question. In response to a request of the Appropriations Committee, the Department recently submitted a report entitled, "Support for EMS Provided by the DHS Office of State and Local Government Coordination and Preparedness" which indicates that under the funding provided for our first responders, the Emergency Medical Services only receives about 4 percent of the total.

What information does the Department have that tells us whether 4 percent is an adequate share to prepare the professionals who will provide emergency medical care to victims at the scene of a potential attack or terrorist event?

Answer. SLGCP provides training, funds for the purchase of equipment, support for the planning and execution of exercises, technical assistance, and other support to assist states, urban areas, and local jurisdictions in preventing, planning for, and responding to acts of terrorism. SLGCP established and maintains several programs that provide these services to emergency responders, including the HSGP, the UASI, and the Assistance to Firefighters Grant Program. SLGCP grant funds can be used to enhance emergency responder capabilities, including EMS, in accordance with the goals and objectives identified in the State or urban area's homeland security strategy. Additionally, fire department-based EMS providers have been, and continue to be, eligible for assistance under the Assistance to Firefighters Grant Program.

The readiness of EMS is vital to ensuring prompt and appropriate emergency care and transportation as a component of the overall response to a terrorist incident. Therefore, it is essential that EMS agencies receive support and assistance from the States and be integrated into planning efforts and working groups to enhance the overall preparedness of state, urban area, and local public safety personnel to prevent, respond to and assist in the recovery from terrorist incidents. SLGCP funds for EMS agencies are allocated through the state's State Administrative Agencies (SAA), in accordance with each state's homeland security strategy. These strategies are based upon comprehensive assessments that address the specific vulnerabilities, threats, capabilities and needs in each state. In recognition of each state's unique threat, need, and vulnerability assessments, the Department does not dictate a specific percentage of funds that should be allocated to supplant EMS services. Instead, the Department supports a distribution strategy capable of addressing the distinctive needs of EMS agencies by allowing specific allocation amounts to be determined at the discretion of each state. However, in recognition of the important role played by EMS providers, the Department issued an Information Bulletin on May 6, 2004. The Information Bulletin reminded States that EMS providers are eligible to receive funding under the State HSGP and UASI programs.

PORT SECURITY GRANT COORDINATION

Question. What coordination is occurring among states, local port authorities and the Captains of the Port, to ensure all vested parties are aware of grant determinations and that the limited resources are maximized when port security grants are made to independent terminal operators?

Answer. As part of the transition of the Port Security Grant (PSG) Program from TSA to SLGCP, the Department has completely redesigned the process to focus on the risk-based prioritization of ports and allocation of the funds to address specific national port security priorities from a port-wide perspective. Redesign of the program was a collaborative process between SLGCP, the U.S. Coast Guard (USCG), the Information Analysis and Infrastructure Protection Directorate (IAIP), the Maritime Administration (MARAD) within DOT, and the American Association of Port Authorities (AAPA), among others. As part of this process the USCG Captain of the Port (COTP) will coordinate a field review of all projects submitted for funding consideration. This field review will be conducted in coordination with the MARAD Region Director, the SAA responsible for the state's Homeland Security Strategy, and appropriate members of each port area's Area Maritime Security Committee (which includes representatives of the local port authorities) to ensure that a port-wide approach to risk reduction is taken and that scarce resources are maximized. Lastly, when determinations of funding have been made, a consolidated list of projects for each port area will be provided to the COTP, MARAD Region Director, SAA, and relevant members of the Area Maritime Security Committee.

TECHNOLOGY TRANSFER

Question. How much of the $50 million appropriated for the Technology Transfer Program has been awarded, to whom and for what projects?

Answer. The Technology Transfer Program is known as the Commercial Equipment Direct Assistance Program (CEDAP). The legislation set aside $10 million for testing and evaluation of commercially available equipment to determine appropriateness for inclusion in the CEDAP program. The remaining $40 million was dedicated to the CEDAP program.

On March 22, 2005, SLGCP officially opened the CEDAP to applications. The applications are competitive and must be consistent with the State homeland security plan. This first pilot test of the program ended May 5, 2005, with applications from 1,500 agencies for $34.4 million in equipment. The first award to 214 agencies of $2.0 million in equipment and training will take place June 15, 2005. (See table below.)

Phase II of the CEDAP program will begin with the opening of the application process in the summer of 2005. Award of the equipment and hands on training for the accepted applicants will take place early in the fall of 2005.

CEDAP AWARDS, ROUND #1—AGENCY BY STATE

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Alabama:				
Alexander City Fire Department	Alexander City	Thermal Imager	Fire Department	$12,500.00
Atmore Police Department	Atmore	Search Camera Victim Locator System	Law Enforcement	14,620.00
Brick Hatton Volunteer Fire Department	Town Creek	Thermal Imager	Fire Department	12,500.00
Calera Fire Department	Calera	Thermal Imager	Fire Department	12,500.00
Calera Police Department	Calera	Search Camera Victim Locator System	Law Enforcement	14,620.00
Cherokee Rescue Squad	Cherokee	Search Camera Victim Locator System	Emergency Medical Services	14,620.00
Cherokee Volunteer Fire Fighters	Cherokee	Thermal Imager	Fire Department	12,500.00
Choctaw County Emergency Management Agency	Butler	Thermal Imager	Emergency Management	12,500.00
Cottonwood Police Department	Cottonwood	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Daphne Police Department	Daphne	Night Vision Kit	Law Enforcement	3,700.00
Georgiana Police Department	Georgiana	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Guntersville Fire/Rescue	Guntersville	Thermal Imager	Fire Department	12,500.00
Jasper Police Department	Jasper	Thermal Imager	Law Enforcement	12,500.00
Margaret Fire and Rescue	Margaret	Thermal Imager	Fire Department	12,500.00
Phoenix City Police Department	Phoenix City	Night Vision Kit	Law Enforcement	3,700.00
Russell County Sheriff's Department	Phoenix City	Night Vision Kit	Public Safety	3,700.00
Alaska:				
Kodiak Police Department	Kodiak	Night Vision Kit	Law Enforcement	3,700.00
Arizona:				
Safford Police Department	Safford	Search Camera Victim Locator System	Law Enforcement	14,620.00
Arkansas:				
Clinton Police Department	Clinton	Thermal Imager	Law Enforcement	12,500.00
Ouachita County Sheriff's Department	Camden	Night Vision Kit	Law Enforcement	3,700.00
Sherwood Police Department	Sherwood	Search Camera Victim Locator System	Law Enforcement	14,620.00
California:				
Greenfield Police Department	Greenfield	Thermal Imager	Law Enforcement	12,500.00
Humboldt County Sheriff's Office	Eureka	Thermal Imager	Law Enforcement	12,500.00
Mariposa County Sheriff's Office	Mariposa	Night Vision Kit	Law Enforcement	3,700.00
Monterey Peninsula Airport Police	Monterey	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
San Rafael Police Department	San Rafael	Thermal Imager	Law Enforcement	12,500.00
Colorado:				
Idaho Springs Police Department	Idaho Springs	Night Vision Kit	Law Enforcement	3,700.00
Manitou Springs Police Department	Manitou Springs	Thermal Imager	Law Enforcement	12,500.00

CEDAP AWARDS, ROUND #1—AGENCY BY STATE—Continued

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Connecticut:				
Mohegan Tribal Fire Department	Uncasville	Night Vision Kit	Public Safety	3,700.00
Putnam Police Department	Putnam	Thermal Imager	Law Enforcement	12,500.00
Torrington Police Department	Torrington	Night Vision Kit	Law Enforcement	3,700.00
Town of Stafford	Stafford	Night Vision Kit	Law Enforcement	3,700.00
Delaware:				
Elsmere Bureau of Police	Elsmere	Thermal Imager	Fire Department	12,500.00
New Castle Police Department	New Castle	Thermal Imager	Law Enforcement	12,500.00
Florida:				
Florida Gulf Coast University Police	Fort Myers	Thermal Imager	Law Enforcement	12,500.00
Havana Police Department	Havana	Thermal Imager	Law Enforcement	12,500.00
Kissimmee Police Department	Kissimmee	Thermal Imager	Law Enforcement	12,500.00
Winter Springs Police Department	Winter Springs	Thermal Imager	Law Enforcement	12,500.00
Georgia:				
Austell Police Department	Austell	Night Vision Kit	Law Enforcement	3,700.00
Jackson County Sheriff's Office	Jefferson	Thermal Imager	Law Enforcement	12,500.00
Idaho:				
Madison County Sheriff's Office	Rexburg	Thermal Imager	Law Enforcement	12,500.00
Rexburg Police Department	Rexburg	Thermal Imager	Law Enforcement	12,500.00
Illinois:				
Elkville Volunteer Fire Department	Dowell	Thermal Imager	Fire Department	12,500.00
Homewood Police Department	Homewood	Thermal Imager	Law Enforcement	12,500.00
Olney Fire Department	Olney	Thermal Imager	Fire Department	12,500.00
Indiana:				
Francesville Volunteer Fire Department	Francesville	Thermal Imager	Fire Department	12,500.00
Hudson Marshal's Office	Hudson	Night Vision Kit	Law Enforcement	3,700.00
Wayne County Sheriff's Office	Richmond	Thermal Imager	Law Enforcement	12,500.00
Iowa:				
Cedar Falls Police Department	Cedar Falls	Search Camera Victim Locator System	Law Enforcement	14,620.00
Eldridge Volunteer Fire Company, Inc.	Eldridge	CEDAP Personal Protective Equipment Kit	Fire Department	4,140.00
Marion County Sheriff's Office	Knoxville	Night Vision Kit	Law Enforcement	3,700.00
Poweshiek County Emergency Management Agency	Grinnell	CEDAP Personal Protective Equipment Kit	HAZMAT	4,140.00
Scott County Sheriff's Office	Davenport	Thermal Imager	Public Safety	12,500.00
Sheldon Police Department	Sheldon	Thermal Imager	Law Enforcement	12,500.00

Kansas:				
Rose Hill Police Department	Rose Hill	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Washington County Sheriff's Department	Washington	Night Vision Kit	Law Enforcement	3,700.00
Kentucky:				
Bourbon County Sheriff's Office	Paris	Thermal Imager	Fire Department	12,500.00
Louisiana:				
District 8 Fire Department	Rayville	Thermal Imager	Fire Department	12,500.00
Grant Parish Sheriff's Office	Colfax	Search Camera Victim Locator System	Law Enforcement	14,620.00
Jackson Parish Sheriff's Department	Jonesboro	Night Vision Kit	Law Enforcement	3,700.00
Lincoln Parish Sheriff's Department	Ruston	Night Vision Kit	Law Enforcement	3,700.00
Richland Parish Sheriff's Office	Rayville	Night Vision Kit	Law Enforcement	3,700.00
Rosepine Police Department	Rosepine	Night Vision Kit	Law Enforcement	3,700.00
St. James Parish Sheriff's Office	Vacherie	Search Camera Victim Locator System	Law Enforcement	14,620.00
West Monroe Police Department	West Monroe	Night Vision Kit	Law Enforcement	3,700.00
Maine:				
Ashland Police Department	Ashland	Night Vision Kit	Law Enforcement	3,700.00
Westbrook Fire Rescue Department	Westbrook	Search Camera Victim Locator System	Fire Department	14,620.00
Massachusetts:				
Burlington Police Department	Burlington	Night Vision Kit	Law Enforcement	3,700.00
Fairhaven Police Department	Fairhaven	Night Vision Kit	Law Enforcement	3,700.00
Gardner Police Department	Gardner	Night Vision Kit	Law Enforcement	3,700.00
Granby Police Department	Granby	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Nantucket Fire Department	Nantucket	Thermal Imager	Fire Department	12,500.00
Norwood Fire Department	Norwood	Thermal Imager	Fire Department	12,500.00
Plymouth Police Department	Plymouth	Thermal Imager	Law Enforcement	12,500.00
Saugus Emergency Management Agency	Saugus	Thermal Imager	Emergency Management	12,500.00
Wayland Police Department	Wayland	Thermal Imager	Law Enforcement	12,500.00
Michigan:				
Gogebic County Emergency Management	Bessemer	Thermal Imager	Emergency Management	12,500.00
Grosse Ile Police Department	Grosse Ile	Thermal Imager	Law Enforcement	12,500.00
Hampton Township Fire Department	Essexville	Thermal Imager	Fire Department	12,500.00
Harper Woods Police Department	Harper Woods	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Kent County Sheriff's Department	Grand Rapids	Night Vision Kit	Law Enforcement	3,700.00
Minnesota:				
Annandale Fire Department	Annandale	Thermal Imager	Fire Department	12,500.00
Cleveland Police Department	Cleveland	Thermal Imager	Law Enforcement	12,500.00
Douglas County Sheriff's Office	Alexandria	Thermal Imager	Law Enforcement	12,500.00
Elk River Police Department	Elk River	Thermal Imager	Law Enforcement	12,500.00
Hector Police Department	Hector	Night Vision Kit	Law Enforcement	3,700.00
Mentor Volunteer Fire and Rescue	Mentor	Night Vision Kit	Fire Department	3,700.00

CEDAP AWARDS, ROUND #1—AGENCY BY STATE—Continued

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Nicollet County Sheriff's Office	St. Peter	Search Camera Victim Locator System	Law Enforcement	14,620.00
Red Lake County Sheriff's Office/OEM	Red Lake Falls	Night Vision Kit	Law Enforcement	3,700.00
Winona County Sheriff's Department	Winona	Thermal Imager	Law Enforcement	12,500.00
Winona Police Department	Winona	Search Camera Victim Locator System	Law Enforcement	14,620.00
Mississippi:				
Clarkdale Fire & Rescue	Meridian	Search Camera Victim Locator System	Fire Department	14,620.00
North Haven Volunteer Fire Department	New Albany	Thermal Imager	Fire Department	12,500.00
Tippah County Sheriff's Department	Ripley	Thermal Imager	Law Enforcement	12,500.00
Missouri:				
Buchanan County Sheriff's Office	St. Joseph	Thermal Imager	Law Enforcement	12,500.00
JasCo Metropolitan Police Department	Oronogo	Night Vision Kit	Law Enforcement	3,700.00
Jonesburg Police Department	Jonesburg	Advanced Portable Detector	Law Enforcement	10,200.00
Kelso Police Department	Kelso	Search Camera Victim Locator System	Law Enforcement	14,620.00
Madison County Sheriff's Department	Fredericktown	Thermal Imager	Law Enforcement	12,500.00
Park Hills Police Department	Park Hills	Thermal Imager	Law Enforcement	12,500.00
Sni Valley Fire Protection District	Oak Grove	Thermal Imager	Fire Department	12,500.00
Terre du Lac Fire and Rescue	Bonne Terre	Thermal Imager	Fire Department	12,500.00
Nebraska:				
Cuming County Sheriff's Office	West Point	Thermal Imager	Law Enforcement	12,500.00
Grand Island Police Department	Grand Island	Night Vision Kit	Law Enforcement	3,700.00
Hall County Sheriff's Department	Grand Island	Thermal Imager	Law Enforcement	12,500.00
Hay Springs Police Department	Hay Springs	Night Vision Kit	Law Enforcement	3,700.00
Keith County Sheriff's Department	Ogallala	Thermal Imager	Law Enforcement	12,500.00
Platte County Sheriff's Department	Columbus	Thermal Imager	Law Enforcement	12,500.00
Wayne County Sheriff's Office	Wayne	Night Vision Kit	Law Enforcement	3,700.00
New Hampshire:				
Allenstown Police Department	Allenstown	Night Vision Kit	Law Enforcement	3,700.00
Durham Police Department	Durham	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
New Jersey:				
Cinnaminson Township Police Department	Cinnaminson	Night Vision Kit	Law Enforcement	3,700.00
Clark Police Department	Clark	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Franklin Township Police Department	Pittstown	Night Vision Kit	Law Enforcement	3,700.00
Glen Ridge Police Department	Glen Ridge	Night Vision Kit	Law Enforcement	3,700.00
Magnolia Police Department	Magnolia	Thermal Imager	Law Enforcement	12,500.00
Ridgefield Police Department	Ridgefield	Thermal Imager	Law Enforcement	12,500.00

Sea Girt Borough Police and Fire Departments	Sea Girt	Advanced Portable Detector	Other	10,200.00
Washington Township Police Department	Robbinsville	Thermal Imager	Law Enforcement	12,500.00
Waterford Township Fire Department	Atco	Thermal Imager	Fire Department	12,500.00
Waterford Township Police Department	Atco	Night Vision Kit	Law Enforcement	3,700.00
New York:				
Harriman Police Department	Harriman	Night Vision Kit	Law Enforcement	3,700.00
Melrose Fire District	Melrose	Thermal Imager	Fire Department	12,500.00
New Windsor Police Department	New Windsor	Thermal Imager	Law Enforcement	12,500.00
North Carolina:				
Beaufort Police Department	Beaufort	Thermal Imager	Law Enforcement	12,500.00
Forest City Fire Department	Forest City	Thermal Imager	Fire Department	12,500.00
McDowell County Emergency Management	Marion	Thermal Imager	Emergency Management	12,500.00
Rocky Mount Police Department	Rocky Mount	Night Vision Kit	Law Enforcement	3,700.00
Rutherfordton Fire Department	Rutherfordton	Thermal Imager	Fire Department	12,500.00
Trent Woods Police Department	Trent Woods	Night Vision Kit	Law Enforcement	3,700.00
North Dakota:				
New England Fire Department	New England	Thermal Imager	Fire Department	12,500.00
Stark County Sheriff's Department	Dickinson	Thermal Imager	Law Enforcement	12,500.00
Ohio:				
Akron Police Department	Akron	Night Vision Kit	Law Enforcement	3,700.00
Beavercreek Police Department	Beavercreek	Night Vision Kit	Law Enforcement	3,700.00
Northwest Ambulance District	Geneva	Advanced Portable Detector	Emergency Medical Services	10,200.00
Oklahoma:				
Enid Fire Department	Enid	Thermal Imager	Fire Department	12,500.00
Marlow Police Department	Marlow	Thermal Imager	Law Enforcement	12,500.00
Owasso Fire Department	Owasso	Thermal Imager	Fire Department	12,500.00
Woodward Police Department	Woodward	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Oregon:				
Cascade Locks Fire & Emergency Medical Services	Cascade Locks	Thermal Imager	Other	12,500.00
Hubbard Police Department	Hubbard	Night Vision Kit	Law Enforcement	3,700.00
Illinois Valley Fire District	Cave Junction	Thermal Imager	Fire Department	12,500.00
Malheur County Sheriff's Office	Vale	Thermal Imager	Law Enforcement	12,500.00
Oakland Rural Fire District	Oakland	Thermal Imager	Fire Department	12,500.00
Turner Police Department	Turner	CEDAP Personal Protective Equipment Kit	Law Enforcement	4,140.00
Turner Rural Fire Protection District	Turner	Thermal Imager	Fire Department	12,500.00
Pennsylvania:				
Bristol Township Police Department	Bristol	Thermal Imager	Law Enforcement	12,500.00
Millersville Borough Police Department	Millersville	Night Vision Kit	Law Enforcement	3,700.00
Wilkes-Barre Police Department	Wilkes-Barre	Thermal Imager	Law Enforcement	12,500.00
Wilkes-Barre Township Police Department	Wilkes-Barre	Thermal Imager	Law Enforcement	12,500.00

CEDAP AWARDS, ROUND #1—AGENCY BY STATE—Continued

[Total Agencies: 214]

State/Agency	City	Technology	Type	Unit Cost
Rhode Island:				
Bristol Police Department	Bristol	Thermal Imager	Law Enforcement	12,500.00
Cumberland Hill Fire District	Cumberland	Thermal Imager	Fire Department	12,500.00
North Smithfield Fire & Rescue Service	North Smithfield	Thermal Imager	Fire Department	12,500.00
Pawtucket Fire Department	Pawtucket	Thermal Imager	Fire Department	12,500.00
South Carolina:				
Hardeeville Fire/Rescue	Hardeeville	Thermal Imager	Fire Department	12,500.00
Tennessee:				
Lenoir City Police Department	Lenoir City	Night Vision Kit	Law Enforcement	3,700.00
Martin Fire Department	Martin	Thermal Imager	Fire Department	12,500.00
Milan Police Department	Milan	Night Vision Kit	Law Enforcement	3,700.00
Texas:				
Arp Marshal's Office	Arp	Thermal Imager	Emergency Management	12,500.00
Bosque County Constable's Office—Precinct 1	Meridian	Night Vision Kit	Law Enforcement	3,700.00
Brownsboro Police Department	Brownsboro	Thermal Imager	Law Enforcement	12,500.00
Clifton Volunteer Fire Department	Clifton	Search Camera Victim Locator System	Fire Department	14,620.00
Cockrell Hill Police Department	Dallas	Night Vision Kit	Law Enforcement	3,700.00
Conroe Fire Department	Conroe	Thermal Imager	Fire Department	12,500.00
Crims Chapel Volunteer Fire Department	Henderson	Thermal Imager	Fire Department	12,500.00
Gainesville Police Department	Gainesville	Night Vision Kit	Law Enforcement	3,700.00
Hillsboro Fire/Rescue	Hillsboro	Thermal Imager	Fire Department	12,500.00
Jacksboro Police Department	Jacksboro	Thermal Imager	Law Enforcement	12,500.00
Marietta Volunteer Fire Department	Marietta	Thermal Imager	Fire Department	12,500.00
Meridian Fire Department	Meridian	Thermal Imager	Fire Department	12,500.00
Valley Mills Police Department	Valley Mills	Thermal Imager	Law Enforcement	12,500.00
Victoria Police Department	Victoria	Advanced Portable Detector	Law Enforcement	10,200.00
Wichita County Texas Emergency Management	Wichita Falls	Search Camera Victim Locator System	Emergency Management	14,620.00
Winters Police Department	Winters	Night Vision Kit	Law Enforcement	3,700.00
Utah:				
Cedar City/Iron County Fire Department	Cedar City	Thermal Imager	Fire Department	12,500.00
Emery County Sheriff's Office	Castle Dale	Night Vision Kit	Law Enforcement	3,700.00
Helper Police Department	Helper	Thermal Imager	Law Enforcement	12,500.00
Morgan County Sheriff's Office	Morgan	Thermal Imager	Law Enforcement	12,500.00
Virginia:				
Amherst County Sheriff's Office	Amherst	Thermal Imager	Law Enforcement	12,500.00

Buena Vista Police Department	Buena Vista	Night Vision Kit	Public Safety	3,700.00
Cumberland County Sheriff's Office	Cumberland	Thermal Imager	Law Enforcement	12,500.00
Emporia Police Department	Emporia	Search Camera Victim Locator System	Law Enforcement	14,620.00
Henry County Sheriff's Office	Martinsville	Night Vision Kit	Law Enforcement	3,700.00
King George Sheriff's Office	King George	Thermal Imager	Law Enforcement	12,500.00
Washington:				
Bainbridge Island Police Department	Bainbridge Island	Thermal Imager	Law Enforcement	12,500.00
Chelan County Sheriff's Office	Wenatchee	Thermal Imager	Law Enforcement	12,500.00
Columbia County Sheriff's Office	Dayton	Night Vision Kit	Law Enforcement	3,700.00
Colville Police Department	Colville	Thermal Imager	Law Enforcement	12,500.00
Colville Tribes Fire Rescue	Nespelem	Thermal Imager	Fire Department	12,500.00
Jefferson County Sheriff's Office	Port Hadlock	Thermal Imager	Law Enforcement	12,500.00
Kettle Falls Police Department	Kettle Falls	Night Vision Kit	Law Enforcement	3,700.00
Lakewood Police Department	Lakewood	Search Camera Victim Locator System	Law Enforcement	14,620.00
Pierce County Fire District 18	Orting	Thermal Imager	Fire Department	12,500.00
San Juan County Sheriff's Office	Eastsound	Night Vision Kit	Fire Department	3,700.00
San Juan Fire District 3	Friday Harbor	Thermal Imager	Law Enforcement	12,500.00
Stevens County Fire District 2	Hunters	Thermal Imager	Fire Department	12,500.00
Stevens County Fire Protection District 1	Clayton	Thermal Imager	Fire Department	12,500.00
Stevens County Sheriff's Ambulance	Colville	Night Vision Kit	Emergency Medical Services	3,700.00
Sumas Police Department	Sumas	Thermal Imager	Law Enforcement	12,500.00
Tumwater Police Department	Tumwater	Night Vision Kit	Law Enforcement	3,700.00
Walla Walla Police Department	Walla Walla	Search Camera Victim Locator System	Law Enforcement	14,620.00
Wisconsin:				
Auburndale Joint Fire and Rescue Department	Auburndale	Thermal Imager	Fire Department	12,500.00
Chippewa Falls Fire and Emergency Services	Chippewa Falls	Thermal Imager	Fire Department	12,500.00
Chippewa Falls Police Department	Chippewa Falls	Night Vision Kit	Law Enforcement	3,700.00
Chippewa Fire District	Chippewa Falls	Thermal Imager	Fire Department	12,500.00
Cottage Grove Police Department	Cottage Grove	Night Vision Kit	Law Enforcement	3,700.00
Fox Valley Metro Police Department	Little Chute	Night Vision Kit	Law Enforcement	3,700.00
Germantown Police Department	Germantown	Night Vision Kit	Law Enforcement	3,700.00
McFarland Police Department	McFarland	Night Vision Kit	Law Enforcement	3,700.00
Mishicot Police Department	Mishicot	Search Camera Victim Locator System	Law Enforcement	14,620.00
Park Falls Police Department	Park Falls	Night Vision Kit	Law Enforcement	3,700.00
Sharon Police Department	Sharon	Thermal Imager	Law Enforcement	12,500.00
Stanley Fire Department	Stanley	Search Camera Victim Locator System	Fire Department	14,620.00
Vernon County Emergency Management	Viroqua	Night Vision Kit	Law Enforcement	3,700.00

Question. What success have come out of the technology transfer program?

Answer. The first award to 214 agencies of $2.0 million in equipment and training took place on May 19, 2005. The second award will take place in the coming weeks. A detailed evaluation is under development to determine the impact and cost effectiveness of the CEDAP program.

CITIZENS CORP

Question. For what, specifically, will the increase of $35 million for Citizens Corp in the fiscal year 2006 President's Request be used?

Answer. The Citizen Corps Program (CCP) is the Department's grass-roots initiative to actively involve all citizens in hometown security through personal preparedness, training, and volunteer service. CCP funds support Citizen Corps Councils with efforts to engage citizens in preventing, preparing for, and responding to all hazards, including planning and evaluation, public education and communication, training, participation in exercises, providing proper equipment to citizens with a role in response, and management of Citizen Corps volunteer programs and activities. State and local governments have embraced the concept of Citizen Corps. They are developing the management capacity of the Councils, conducting public education, providing training for citizens, and engaging citizens through volunteer programs. However, there is a need to expand this effort to ensure that citizens are integrated in all aspects of State and local government preparedness, response and recovery and to support more significant community outreach through schools, private and public sector worksites, faith-based organizations, recreational outlets, and local media. The requested $50 million is critical to meet the demand and build the capacity of preparing, training, and involving citizens. In the end, this will result in the development of a fully-prepared community, with citizens who are fully aware, trained and practiced on how to detect, deter, prepare for, and respond to all hazards and threats.

BEST PRACTICES

Question. As the Office of State and Local Government Coordination and Preparedness discovers lessons learned and best practices across the Nation regarding procurement and allocation of grant funding, are those practices being collected and made available for State and local governments to benefit?

Answer. SLGCP currently has several avenues to identify and share grant-related best practices and lessons learned with its State and local grantees.

—The office has analyzed the states' and territories' narrative on management capabilities responses included in the fiscal year 2005 HSGP applications, including information on allocation of grant funding. SLGCP will provide each respondent with a written overview summary analysis that highlights best management practices and lessons learned. This overview will allow States to learn about approaches that are working successfully in other states. In addition to the overview, SLGCP will also provide a state-specific analysis of the management capabilities outlined in the applications.

—SLGCP is developing a Program Management Handbook that includes guidelines for building strong program management infrastructures. These guidelines have been written to provide a common, flexible framework with potential for customization at the state, regional, and local levels. Best practices in program management will be collected and disseminated to support the implementation of the capabilities outlined in the Handbook.

—ODP is exploring ways to provide procurement assistance including identification and dissemination of procurement best practices to help States develop streamlined procurement practices. Currently under development is procurement technical assistance including informational materials, tools and templates, and customized on-site guidance.

AIRBORNE RAPID IMAGING FOR EMERGENCY SUPPORT

Question. In the aftermath of the September 11 terrorist attacks on the World Trade Center, the State of New York utilized a technology that provided maps to first responders showing location, elevation, and temperature ranges of features on the ground within 8–10 hours after data collection. The Department of Homeland Security's Office of State and local Government Coordination and Preparedness provided $3 million in 2004 to demonstrate and further improve this technology by reducing turn around time through a system called the Airborne Rapid Imaging for Emergency Support (ARIES).

What were the results of the ARIES flight demonstration that was conducted last November?

Answer. The Airborne Rapid Imaging for Emergency Support (ARIES) program was a DHS-funded initiative to explore the technical feasibility of providing near real-time map-quality imagery for first responders in the event of a crisis. The program began in the spring of 2004 and culminated with a technical demonstration on November 17, 2004 at Picatinny Arsenal in New Jersey. The objectives of the demonstration were as follows:

—Demonstrate the capacity to obtain digital imagery rapidly using commercial aircraft in a simulated emergency event.
—Downlink this imagery directly from the aircraft to a receiving station using micro millimeter wave technology.
—Process the raw, uncorrected imagery in a portable environment for use by existing DHS systems within 3 hours of acquisition.
—Distribute the imagery to multiple agencies for emergency needs.
—Provide on-site visualization, tracking, and information gathering capabilities to assist with any emergency response requirements.

The demonstration satisfied the technical criteria for four of the five components. Distribution of the imagery was not successfully demonstrated. This was a technical demonstration that did not address the utility of ARIES' orthorectified imagery products to emergency responders.

Overall, the ARIES program proved the technical feasibility of the concept. A final program report including a costing analysis of the ARIES concept was conducted by the Institute for Defense Analysis. The report is in the final review process and will be made available upon completion.

Question. What is the current capability in Federal, state, or local government organizations or private industry to provide integrated digital imagery, lidar, and thermal information to first responders?

Answer. Many types of imagery, acquired for particular uses, are available commercially to support first responders. The capability of various organizations to deliver this imagery directly to first responders varies significantly from State to state. However, the capability of first responders to receive it and do sophisticated analysis is limited because there is no end-to-end system in place to acquire process and deliver imaging products to the first response community. The DHS Geospatial Management Office (GMO) is currently conducting pilot programs to demonstrate delivery of geospatial products to first responders using wireless hand held devices.

Question. What is the Department's need and plan to advance and utilize this technology?

Answer. According to the DHS GMO, the simultaneous collection, processing and integration of Digital Electro-optical (EO) Imagery, Light Detection and Ranging (LIDAR) elevation data and Thermal Infrared (TIR) Imagery from a single aerial platform was demonstrated in the ARIES pilot. The ARIES demonstration provided a unique capability determined to be necessary in the aftermath of September 11. Imaging technologies are collected and used by Federal, State or local organizations in a variety of mapping applications or special studies. Currently, however, the acquisition, dissemination and use of airborne and space-borne sensor information for emergency response are mostly uncoordinated among levels of government, across jurisdictions and between mission areas.

The DHS GMO is responsible for providing leadership and coordination in meeting the geospatial information requirements of those responsible for planning, prevention, mitigation, assessment and response to emergencies, critical infrastructure protection, and other functions of the Department. The GMO is working with the DHS components as well as other Federal, State and local organizations to understand the geospatial information needed to support their missions. The GMO developed the Geospatial User Needs Assessment Report which identified many of the needs. The GMO has also produced and is maintaining the Geospatial View of the Geospatial Enterprise Architecture which is a current view of the as-is and target geospatial information technology architecture for DHS. The DHS Geospatial Architecture view is referenced in the fiscal year 2005 HSGP and is being used as a model for the emerging Geospatial Profile. As the DHS and HLS architecture mature, rapid geospatial imagery acquisition requirements will be identified and services will be acquired.

HAZARD MITIGATION

Question. The Hazard Mitigation Grant Program provides critical funding to States following a declared natural disaster to assist them in reducing future disaster losses. The funding is an amount equivalent to a percentage of eligible FEMA funds. The funds provided are 75 percent Federal and 25 percent local or State. Since the passage in December 2000 of the Disaster Mitigation Act which amended

the Stafford Disaster Relief Act, FEMA has encouraged States to put forth the additional effort required to obtain an approved enhanced plan. Those with an enhanced plan would be eligible for an amount equivalent to up to 20 percent of eligible FEMA funds. Based on this incentive numerous States are working to obtain this goal. The fiscal year 2006 President's Budget proposes language to reduce the percentage to up to 12.5 percent.

Since this incentive has been in the law for 4 years, why are you requesting this change now that some States have put forth significant commitment of already overburdened resources to achieve enhanced status?

Answer. The President's Budget request preserves the 5 percent incentive for developing enhanced mitigation plans. The Hazard Mitigation Grant Program (HMGP) now uses a 7.5-percent multiplier to calculate the amount of mitigation money available to a State after a disaster declaration, when the State has an approved basic mitigation plan. When the State has an approved enhanced mitigation plan, it is eligible for up to 12.5 percent. Both the Administration and Congress agreed to the 7.5 percent basic formula, which was changed from 15 percent when Congress created the Pre-disaster Mitigation (PDM) program to provide additional funding for mitigation activities on a nationally competitive basis.

The incentive was 5 percent when the program used a 15 percent baseline and when HMGP represented the primary means for States to receive Federal mitigation funds. The incentive remains 5 percent now. Under the old plan, only the States in which a disaster was declared were eligible. However, the availability of PDM grant funds allows the States to compete for mitigation funds without a Presidential disaster declaration. The budget request of up to 12.5 percent HMGP for the States with enhanced mitigation plans preserves the 5 percentage point incentive authorized in the Disaster Mitigation Act of 2000.

Question. Which States have approved plans and which States are in the process of working on enhanced plans?

Answer. All 50 States now have approved State Mitigation Plans. In addition, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, American Samoa, Guam, the Commonwealth of the Northern Mariana Islands, and the Republic of the Marshall Islands have approved state-level mitigation plans. (The Federated States of Micronesia is the only non-Tribal jurisdiction without an approved plan. FEMA Region IX expects to be able to approve it soon.)

There are currently four States with approved enhanced mitigation plans: Missouri, Ohio, Oklahoma, and Washington. FEMA has recently reviewed enhanced plans from Maryland and Pennsylvania; however, they require revision prior to approval. The following States have advised FEMA that they may submit enhanced plans for review and approval within the next 6 months: Alabama, Florida, Georgia, Iowa, Louisiana, Minnesota, Mississippi, North Carolina, Oregon, Texas, Virginia, and Wisconsin. Arizona, California, Delaware, North Dakota, and Utah have expressed interest in developing enhanced mitigation plans, but, to date, such plans have not been received.

Question. Were the States advised that you intended to reduce the incentive?

Answer. The fiscal year 2006 President's Budget is the first time that a specific percentage, other than 20 percent, has been communicated to the States working on enhanced plans. The incentive for an enhanced plan, however, remains 5 percent.

FLOOD MAP MODERNIZATION

Question. What is the schedule, by state, for implementation of the Flood Map Modernization Program?

Answer. The schedule varies from State to State and changes from year to year. FEMA has developed a strong business planning process in which it works with the States and with other significant mapping partners to identify and schedule mapping projects jointly. FEMA then works with its partners to execute the plan based on the funding appropriated and makes adjustments twice a year to align schedules with current realities. FEMA balances stakeholder input with national and regional flood mapping needs to develop a nationwide plan for flood map update schedules and anticipated budgets. FEMA used stakeholder input to develop the initial plan, and received additional feedback on the plan that will be addressed in future updates. The current Multi-year Flood Hazard Identification Plan (MHIP), detailing the 5 year schedule and budget for developing the updated flood hazard data and maps, can be accessed online at http://www.fema.gov/fhm/mh__main.shtm.

Question. Are we on track to complete this project within the projected timeframe of completion in fiscal year 2008 within the budget that has been appropriated and requested?

Answer. FEMA is on track to complete the project by 2010, should the funding requested through 2008 be provided. That is, studies funded in 2008 are expected to be complete by 2010. The digital flood hazard data will meet quality standards contained in the MHIP. However, stakeholders have identified additional engineering requirements beyond what can be accomplished within this project. Data on these additional engineering requirements are being collected as FEMA coordinates with States and communities during the nationwide mapping effort. These data will provide the basis for evaluating future resource needs.

Question. What sort of cooperation is happening with State and local governments?

Answer. The map modernization effort is built upon constant collaboration between FEMA Headquarters and FEMA Regions I–X, the States and local entities, and the business planning process facilitates this collaboration. Many FEMA mapping partners are contributing not only to the flood map production process, but to the planning process as well. In fiscal year 2003 and fiscal year 2004, FEMA provided more than $92 million directly to its Cooperating Technical Partners (CTPs) to develop flood map data in support of map modernization. Also, in 2002, as part of its broader effort to incorporate local, state, and regional involvement in flood mapping, FEMA asked the states, territories, and some CTPs with multi-jurisdictional responsibility for floodplain management to prepare map modernization plans. The plans included extensive flood mapping needs assessments that were developed pursuant to FEMA and other criteria. In early fiscal year 2004, FEMA made funds available through the Flood Map Modernization Management Support (FMMMS) program to these same entities to upgrade and update their plans. FEMA received a total of 55 plans covering 48 States and four of the five water management districts in Florida. FEMA also received plans from the District of Columbia and two Territories.

The FMMMS program, with more than 50 partners, provides a means to ensure that partners can support Flood Map Modernization through administration and management activities. These activities, although not directly resulting in the production of a flood map, increase partners' investment and capability to manage their flood hazard data, strongly bolster the efforts of mapping partners, and ensure a tailored, local focus within a national program. Two of the most vital outcomes of FMMMS are the partners' ability to review program planning policy and guidance and their identification of needs as a part of their business planning process.

Question. What will the maintenance cost of this program be once the modernization piece is completed?

Answer. FEMA is currently estimating maintenance costs and will provide this information to the Office of Management and Budget as scheduled. The strong partnerships, business planning processes, and flood mapping technologies deployed as part of Flood Map Modernization will allow FEMA to improve its estimated maintenance costs as the program draws to completion. FEMA will continue to work with the States and communities to define the most efficient and effective approach for providing and maintaining up-to-date flood hazard information for the nation.

CERRO GRANDE FIRE CLAIMS

Question. What is the unobligated balance of the Cerro Grande fire claims fund?

Answer. As of April 30, 2005, the unobligated balance of the Cerro Grande fire claims fund is $36,559,305.

Question. Is there a deadline for claims? If so, what is it?

Answer. The deadline for filing claims (other than mitigation claims) with the Office of Cerro Grande Fire Claims was August 28, 2002. The deadline for filing mitigation claims was August 28, 2003.

Question. If it has passed, what is the remaining balance of the fund?

Answer. As of April 30, 2005, the remaining unobligated balance of the Cerro Grande fire claims fund is $36,559,305.

Question. How many claims totaling how much are left to be resolved and what is the timeline for resolving those claims?

Answer. FEMA has successfully processed 21,453 claims, including all administrative appeals. There are two claims left to be resolved. Those claims, totaling $5,249,866, were filed in the United States District Court for New Mexico. The resolution of these two cases depends on the schedule of the United States District Court. All of the 4,529 subrogation claims have been processed, and 70 percent of each of those claims has been paid, leaving $34,509,270 as the remaining subrogation liability. The subrogation claims will be paid with funds remaining after the adjudication of the two claims in Federal Court.

PRE-DISASTER MITIGATION GRANTS

Question. Last year the Conferees expressed concern over the slow progress in awarding fiscal year 2003 Pre-disaster Mitigation Grants and over the unobligated balances that remained in the program. How much fiscal year 2004 funding has been released to date and how much remains unobligated in the program?

Answer. To date, FEMA has not released any fiscal year 2004 competitive grant funding ($131 million). Since the PDM funds are available until expended, FEMA is combining the remaining fiscal year 2003 funds with the fiscal year 2004 funds and with the fiscal year 2005 appropriation into a streamlined fiscal year 2005 PDM competitive grant program. Of the fiscal year 2004 appropriation of $149 million, a total of $137 million (competitive grants, administrative, and miscellaneous funding) remains unobligated.

Question. For fiscal year 2005 funds, why is it taking so long to distribute the funds and how can the program be expedited?

Answer. After completing the first competitive PDM process, FEMA began awarding the fiscal year 2003 grants in April 2004. The fiscal year 2003 appropriation, authorized in February 2003, directed FEMA to implement a PDM grant program in three parts: (1) a nationally competitive PDM grant program for state, territory, local government, and Indian tribal government projects and plans; (2) a nationally competitive PDM grant program for disaster-resistant university projects and plans; and (3) a one-time planning grant allocation to the states and territories. The PDM grants are awarded based on the results of a three-phase competition—eligibility and completeness review, technical evaluation, and national evaluation team review. The applications are ranked and announced, and subsequently, the applicants are notified that their application has been selected for funding. Once this takes place, the grant award process can begin. The majority of the fiscal year 2003 funds have been awarded; however, an additional $18.5 million will be awarded when ongoing Federally required environmental and historic preservation compliance reviews are complete. FEMA anticipates that this will be no later than the end of fiscal year 2005. At that point, FEMA will have funded all eligible fiscal year 2003 grant applications and approximately $11 million in fiscal year 2003 funds will remain.

In response to the announcement of funds available for fiscal year 2005, FEMA received 821 applications totaling nearly $517 million. FEMA conducted eligibility and completeness reviews in March 2005. Technical reviews in the areas of engineering, cost effectiveness, and environmental and historic preservation were conducted in March and April 2005. The National Evaluation will be conducted May 17-June 3, 2005. Representatives from 27 states, 3 tribes, and 1 territory will participate in the National Evaluation process.

Based on the eligibility, completeness, and technical reviews completed to date, FEMA expects that the selection of grants for award will be completed in June, after which pre-award activities and the obligation of grant awards will begin. Grants will be selected so that ultimately, all funds from fiscal year 2005 and prior years will be obligated.

Federal environmental and historic preservation compliance requirements for project grants, as well as state-level grant processing requirements, are significant factors that can delay the obligation of grant funds to selected grantees. FEMA will work with grantees to complete these requirements expeditiously; however, for those grants that cannot be obligated in fiscal year 2005, FEMA will work to complete the requirements and to obligate the grant funds as early as possible in fiscal year 2006.

FEMA PERSONNEL

Question. Recently FEMA has experienced a large number of vacancies. In fiscal year 2004 and to date in fiscal year 2005 how many vacancies has FEMA experienced in headquarters and in the regions?

Answer. At the end of fiscal year 2004, there were approximately 357 vacancies agency-wide (not including Stafford Act employees). By mid-year of fiscal year 2005, FEMA had approximately 342 vacancies agency-wide.

Question. Were any of those vacancies eliminated or transferred to other parts of DHS?

Answer. Yes, some of the vacancies were transferred to the SLGCP at the start of fiscal year 2005.

Question. Is so, what is the total number eliminated, and the total number transferred and to where?

Answer. Sixteen vacancies were transferred to SLGCP at the start of fiscal year 2005.

Question. How many vacancies does FEMA have as of April 20, 2005?

Answer. As of April 20, 2005, FEMA has approximately 342 vacancies.

Question. What is the current plan at FEMA for filling vacancies?

Answer. FEMA will continue to fill vacancies and to maintain staffing levels sufficient to sustain its mission.

Question. How has the vacancy of so many positions affected the ability to prepare and respond to disasters?

Answer. FEMA still is able to maintain its mission capability.

IA'S ROLE IN INTELLIGENCE COMMUNITY

Question. In February 2004, the DHS IG noted that the mission of the IAIP Risk Assessment Division (RAD) overlaps in many ways with the Terrorist Threat Integration Center (TTIC), now called the National Counterterrorism Center. The TTIC was created through executive order in 2003. In August 2004, the IG noted that DHS is not playing a lead role in consolidating terrorist watch list information even though the Homeland Security Act called for DHS to play a major role in watch list consolidation. In December of 2004, the Intelligence Reform and Terrorism Prevention Act was signed by the President making sweeping changes in the intelligence community.

With the Intelligence Reform Act and other executive orders stripping away most of the responsibilities of IA and placing them with the National Counterterrorism Center (NCTC) and the Terrorist Screening Center, what role does IA play in the intelligence community?

Answer.

The Role of DHS Office of Information Analysis in the Intelligence Community

DHS Office of Information Analysis (IA) plays a leading role in the intelligence community for homeland security intelligence. The Office provides border, infrastructure, maritime and domestic threat analysis; fuses unique information from our components and our non-traditional stakeholders; and serves as the primary intelligence information provider to state, local, territorial and tribal governments and the private sector, as well as their advocate for intelligence information within the intelligence community. As I announced on July 12, 2005, I am committed to enhancing this role.

DHS IA's role as a leader of homeland security intelligence within the intelligence community is likewise enhanced by the IRTPA 2004 and other executive orders; the greater integration of the intelligence community as a result of IRTPA 2004 will strengthen the ability of DHS IA to carry out its mission.

IRTPA 2004 and the Integration of the Intelligence Community

DHS IA is aggressively integrating into the intelligence community to ensure we can maximally contribute to the nation's security, especially in our unique areas of expertise (producing unique analysis and providing unique information), and to ensure we are able to most effectively leverage the expertise and support of the intelligence community on behalf of the Homeland Security mission and its stakeholders, especially those non-traditional stakeholders such as State, local, territorial, and tribal governments and the private sector (with whom we have unique partnerships).

Integrating DHS IA Unique Analytic Expertise into the Intelligence Community

DHS IA has "forward deployed" DHS intelligence analysts to our intelligence community partners, to include the National Counterterrorism Center (NCTC), the Federal Bureau of Investigation, and to non-intelligence community members such as the TSC.

These seasoned analysts are able to ensure our intelligence community partners have the benefit of our unique DHS analytic expertise in Border Security Intelligence, Infrastructure Security Intelligence, Maritime Security Intelligence (esp. through our Homeland Infrastructure Threat and Risk Assessment Center), and Domestic Threat Intelligence.

We frequently collaborate with our partners when expertise is required in our unique analytic areas and we are fully engaged in ongoing community efforts to develop community production plans reflective of an efficient application of the community's resources. For example, DHS IA is fully participating in the NCTC led effort to develop a communitywide counterterrorism production plan; we are taking the lead in those areas that make use of our unique DHS analytic areas (borders, infrastructure, maritime and domestic threat, as appropriate) and partnering with other organizations on those topics that will be strengthen by including our experts' input.

Working with NCTC and TSC on Analysis

DHS IA has been a strong partner in NCTC since its inception as the Terrorist Threat Integration Center in January 2003. On a daily basis we levy the expertise resident in the NCTC to answer the needs of our customers—we focus on ensuring the best counterterrorism analysis in the government is put into a form, context and classification that is useful for our state, local, territorial and tribal governments and private sector partners. At the same time, we provide our substantial expertise to the NCTC on areas where we are the experts: borders, infrastructure, maritime, and domestic threat analysis. The result of this partnership is that we work together on many joint products—bringing the best expertise in the government to bear on behalf of our customers.

DHS IA took a lead role in helping stand up the TSC, providing staff and support (to include a senior manager). Our experienced analysts in the TSC help ensure the success of its vital work in watchlist consolidation.

DHS IA also conducts a valuable alternative analysis program; our Red Cell provides alternative analytic perspective to complement—and challenge—NCTC and others findings. Our Red Cell has received compliments for its insightful and adventurous thought—and this work is an essential component of the alternative analytic capability required under IRTPA 2004.

Integrating DHS IA Unique Information into the Intelligence Community

In parallel with our efforts to integrate DHS unique analytic expertise into the intelligence community, we are also moving forward in ensuring our vast DHS unique information holdings are made available to the intelligence community through direct access and quality reporting.

DHS has vast information holdings, unique to this department, either as a result of our operational elements' investigations and enforcement operations or as a result of our unique position as the primary interface between the Federal Government and the State, local, territorial and tribal governments and private sector.

DHS IA is working to ensure analysts throughout the intelligence community have access to our information holdings, while respecting the privacy and civil liberties of our citizens. In several cases, the Department has made operational elements' data holdings directly available to partner organizations in the intelligence community. In addition, DHS IA is establishing a reports officer program, focused on drawing information out of the department's information holdings and placing them into traditional intelligence community channels, through the Intelligence Information Reports vehicle. DHS IA has deployed trained reports officers into key departmental operational nodes to report counterterrorism information derived from border enforcement efforts and immigration investigations to the intelligence community. In the future, DHS IA will deploy trained reports officers throughout the components—and out into State and Local Fusion Centers—to ensure the all the department's relevant information is made available to those who need it, in a timely manner and in the channels analysts in the intelligence community are comfortable with and expect to receive reporting.

Integrating DHS IA Unique Partnerships into the Intelligence Community

DHS IA has been charged to be the primary Federal Government intelligence information provider to the State, local, territorial, and tribal governments and the private sector (a responsibility re-emphasized by IRTPA 2004)—and to be their advocate within the intelligence community. On a daily basis we are integrating our support for these customers into the larger intelligence community by working to ensure the free flow of information and products from the intelligence community out to our customers, by providing actionable intelligence, and by contextualizing intelligence to explain the product to our customers in terms they understand and working with our partners to produce the reports at the classification levels our stakeholders can use.

We are also continually working to ensure our customers' requirements—whether they are for information or for finished analytic production—are represented in the intelligence community requirements statements, collection decks, and production plans. Our work in integrating the homeland security intelligence requirements of the state, local, territorial, and tribal governments and the private sector into the intelligence community requirements system is the first time these requirements have been systematically included and advocated for in the intelligence community.

IRTPA 2004 and DHS IA Departmental Responsibilities

In addition to our lead role for homeland security intelligence within the intelligence community, DHS IA maintains several key departmental support respon-

sibilities—including a new role of leading and managing the departmental intelligence activities.

Some of these key departmental roles include:

—Providing direct support to the Secretary and department senior staff for policy, programmatic, and operational decision making.

—Developing the plans, programs and policies required to build a unified, integrated DHS intelligence capability, which the Secretary has said will lie at the heart of the department's risk-based approach to securing the homeland.

—Supporting the Homeland Security Advisory System (HSAS). IA will continue to provide specific intelligence to the Secretary and the White House to enable timely changes in the threat level and support dissemination of this information to stakeholders. We will contribute to the function of Indications & Warning (I&W) in partnership with the HSOC.

—Building out of the intelligence infrastructure for DHS headquarters.

—Developing an Education, Training, and Career Workforce Management Program for DHS analysts and intelligence professionals.

Finally, early reviews by the DHS OIG and concerns resulting from the changing roles and responsibilities of the NCTC and other organizations due to IRTPA 2004 and other executive orders are not reflective of the successes DHS IA has demonstrated as a leader within the intelligence community for homeland security intelligence. As stated above, our value added comes in our unique data and analytic expertise (border, infrastructure, maritime, and domestic threat analysis—analysis that has distinguished itself on several occasions and led the community toward the appropriate threat characterization), in providing our unique information (information never before available to the intelligence community and by which we have already contributed to successes in other agencies), and in partnering with our stakeholders—especially in our unique role as the primary Federal Government intelligence information provider to the state, local, territorial, and tribal governments and the private sector and in our role as their advocate within the intelligence community.

We remain focused on our mission of leading the DHS intelligence activities in support of the department and its components, and for the full benefit of the state, local, territorial, and tribal governments and the private sector, to secure the homeland, defend our citizenry, and protect our critical infrastructure.

Question. What role does the Homeland Security Operations Center (HSOC) serve in comparison to the NCTC?

Answer. In contrast to the NCTC, the HSOC provides general domestic situational awareness, a common operational picture, and support to the IIMG and DHS Leadership, as well as acting as the primary conduit for the White House Situation Room and IIMG for domestic situational awareness. The HSOC will continue to collect domestic related suspicious activity reports, look at domestic terror threats and natural disasters, focusing efforts domestically. HSOC is the lead conduit to State and local agencies.

Question. The FTE levels authorized for IAIP appear to be based on the larger role in intelligence gathering and analysis that was envisioned when IAIP was established. What is the justification to carry such a high number of FTE for intelligence analysis now that many functions envisioned by the Homeland Security Act have been placed at other agencies?

Answer. IAIP's mission is an entirely new one, and it is a manpower-intensive effort owing to the vast size and scope of the threats to the homeland. IAIP is performing an intelligence mission never before attempted, and it is a mission that includes Federal, state, local, tribal entities as well as privately-held interests. Additionally, IAIP is responsible for intelligence pertaining to securing the borders of the United States, which is in itself an enormous undertaking. DHS and IAIP have been given the mission of producing intelligence analysis and products that simply did not exist before, and to do so with a "target set" that is staggering in its size and complexity. While the need to conserve resources is clear, the need to perform the analyses needed to ensure that our Homeland is prepared to detect, intercept, withstand, and, if necessary, recover from a terrorist attack is even more vital.

CHEMICAL SECURITY

Question. Last year, I asked Secretary Ridge about his plans to address security at chemical plants and he told me that the private sector was taking care of it. Yet, the Department has no benchmarks to determine whether the private sector is taking steps to secure its facilities. In response to this apparent gap in our security, last year, I asked GAO to determine what steps are being taken by the private sector to protect the American people. The GAO concluded that for 93 percent of the

industry, it is uncertain whether facilities are improving security at all. Only 1,100 of the 15,000 chemical facilities identified by the Department of Homeland Security are known to adhere to voluntary industry security procedures.

It has been more than 2 years since the GAO urged the EPA and DHS to develop a comprehensive strategy for the protection of our chemical plants. Yet, little has been done.

What are your plans to enhance security for the chemical sector?

Answer. As part of the development of the NIPP, the Office of Infrastructure Protection (IP) has been tasked with authoring the Chemical Sector Specific Plan (SSP), which will outline the strategic guidance for securing the Chemical Sector.

While the Chemical SSP is being developed, DHS continues to work within the Chemical Sector to enhance overall protective capability through several ongoing initiatives. To help guide the resource targeting of these initiatives, the Department is applying a risk management process that examines the likelihood of a given event and its potential consequences. This approach allows for the Department's protective efforts to be directed at those chemical facilities posing the greatest potential danger to the American public. Examples of these protective efforts include the following:

—*Site Assistance Visits (SAVs).*—SAVs are visits to critical infrastructure facilities by DHS protective security professionals in conjunction with subject-matter experts and local law enforcement (LLE) to assist asset owner/operators in assessing vulnerabilities at their facilities. To date, SAVs have been conducted at 38 chemical facilities.

—*Buffer Zone Protection Plans (BZPPs).*—BZPPs identify and recommend security measures for the area surrounding a facility (the "Buffer Zone"), making it more difficult to plan or launch an attack. DHS trains LLE personnel on how to assess Buffer Zone security and provides a standardized template for use in the creation of a BZPP. To date, DHS has received BZPPs for 111 chemical facilities, with BZPPs expected to be completed for the 289 highest-risk chemical facilities by the end of fiscal year 2005. In conjunction with the BZPP program, $14.5 million in grants have been provided to first preventers responsible for the protection of chemical facilities

—*Educational Reports.*—Based on data gathered from SAVs and BZPPs, DHS has developed three types of educational reports for use by LLE and asset owner/operators to learn how to better secure CI/KR assets. Characteristics and Common Vulnerabilities reports (CVs) identify common characteristics and vulnerabilities at specific types of CI/KR. Potential Indicators of Terrorist Activity reports (PIs) provide information on how to detect terrorist activity in areas surrounding CI/KR. Protective Measure (PM) reports identify best practices and other protective measures for use at specific CI/KR types. CVs and PIs have been developed for Chemical Facilities, Chemical Storage Facilities, and Chemical and Hazardous Materials Transportation. A PM report has been developed for the Chemical and Hazardous Materials Industry.

—*Facility Security Assessments/Facility Security Plans (FSAs/FSPs).*—Pursuant to the Maritime Transportation Security Act of 2002 (MTSA), owners of chemical facilities located along waterways are required to complete FSAs and FSPs and submit them to the USCG for review and approval. FSPs must include security measures and procedures for responding to security threats. To date, USCG personnel have visited over 230 chemical facilities under the MTSA.

—*Risk Analysis and Management for Critical Asset Protection (RAMCAP).*—DHS, in conjunction with the American Society for Mechanical Engineers, is developing the RAMCAP, a risk assessment methodology that will allow asset owners/operators to assess the security of their critical assets. Results from RAMCAP assessments will allow comparison of assets from across sectors, allowing for better prioritization of national CI protective efforts. The Chemical Sector module will be completed by the end of the second quarter of fiscal year 2005.

—*Webcams.*—Web-based cameras have been installed at ten high-risk chemical facilities in order to enable LLE and DHS to conduct remote surveillance of the buffer zone surrounding each facility during elevated threat levels.

—*Tabletop Exercises.*—As part of DHS-IP's Exercise Program, tabletop exercises have been conducted at six chemical facilities. The findings from these exercises are compiled in After Action Reports which serve as a basis for planning future exercises; upgrading security plans and operating procedures; and taking corrective actions.

—*TIH Rail Security.*—DHS, in conjunction with DOT, is supporting a variety of efforts to improve security for Toxic-by-Inhalation Hazards (TIH) rail shipments. These efforts include studying ways to make HAZMAT rail cars less identifiable; conducting vulnerability assessments for the high-risk urban areas

where the largest quantities of TIH chemicals move by rail; a DC Rail Pilot Project involving a "virtual fence" with various sensors and monitors to help secure the DC rail corridor from potential incidents involving HAZMAT; and establishing TIH HAZMAT teams in the DC area.

—*Training.*—DHS provides various training courses to asset owner/operators, State and local government officials, and LLE agencies responsible for the protection of chemical facilities. Such courses include: Terrorism Awareness and Prevention; Advanced Bomb Technician Training; Surveillance Detection; SWAT Operations; and Underwater Hazardous Device Search Training.

—*Private Sector Initiatives.*—In addition to protective activities led by DHS or other Federal entities, asset owner/operators in the Chemical Sector are voluntarily undertaking a variety of security initiatives. Chief among these is performance of self-assessments using the Responsible Care® Security Code (Security Code). This code, developed by one of the Chemical Sector's largest trade associations, is designed to help chemical facilities improve their security using a risk-based approach to identify, assess, and address vulnerabilities; prevent or mitigate incidents; and enhance training and response capabilities. Implementation of the Security Code is a prerequisite for membership in some of the sector's largest industry associations. Recently, DHS reached a tentative third party verification agreement with two of these associations (the American Chemistry Council and the Chlorine Institute).

Question. Will legislation be proposed to Congress that sets security standards across the industry?

Answer. At this time, our non-regulatory partnerships with industry are producing results. However, DHS has concluded that the existing patchwork of authorities does not permit us to regulate the industry effectively. Accordingly, DHS has agreed to work with Congress to assess the need for a carefully measured, risk-based regulatory regime in the chemical sector designed to close the existing gaps and develop enforceable performance standards to reduce risk across the chemical sector.

Question. Do you agree that the Department must establish benchmarks to assess both the private sector's and Federal Government's role in securing the chemical sector?

Answer. DHS believes facility chem site security should be based on reasonable, clear, equitable performance standards. Enforceable performance standards should be based on the types and severity of potential threats posed by terrorists, and facilities should have the flexibility to select among appropriate site-specific security measures that will effectively address those threats.

BUFFER ZONE PROTECTION PLANS

Question. DHS recently released $92 million in Buffer Zone Protection Plan grants. Of the 1,849 grants, provide a chart that shows the distribution of grants and the funding by critical infrastructure sector.

Answer. Please see table below.

BREAKDOWN OF BZPPS BY SECTOR FOR FISCAL YEAR 2004–2005

SECTOR	Number of sites [1]	Percent of sites	Approx. funding [2]
Agriculture & Food	5	0.27	$250,000
Banking & Finance	41	2.20	2,050,000
Chemical & Hazardous Materials Industry	272	14.62	13,199,870
Commercial Assets	880	47.29	43,592,631
Dams	7	0.38	350,000
Defense Industrial Base	6	0.32	300,000
Emergency Services	5	0.27	202,975
Energy	213	11.45	10,550,954
Government Facilities	142	8.28	7,100,000
Information Technology	5	0.27	250,000
National Monuments & Icons	10	0.54	500,000
Nuclear Power Plants	92	4.94	4,423,802
Postal Shipping	2	0.11	100,000
Public Health	23	1.24	1,117,506
Telecommunications	5	0.27	250,000
Transportation	98	5.27	4,836,168
Water	43	2.31	2,150,000

BREAKDOWN OF BZPPS BY SECTOR FOR FISCAL YEAR 2004–2005—Continued

SECTOR	Number of sites [1]	Percent of sites	Approx. funding [2]
TOTALS	1,849	100.00	$91,223,906

[1] The exact composition of the fiscal year 2004–05 BZPP list is still evolving; the current sector breakout is a snapshot, but will not change substantially.

[2] Subject to prioritization decisions of 18 States and 1 territory that have elected to prioritize their assets, an exact sector breakdown is not currently available. A total of $91,315,793 is available under the grant program.

Question. Does DHS plan to broaden the criteria for receiving grants to include the gross consequence of an attack and other vulnerabilities?

Answer. In determining where to target its protection resources, DHS applies a risk management process that examines the likelihood of attack and its potential consequences. This approach allows the department's protective efforts to be directed at those facilities posing the greatest potential danger to the public. DHS is continuing to improve data collection in support of risk analysis, and to refine our risk assessment methodologies to ensure resources are being spent where they are most needed.

MANAGEMENT & ADMINISTRATION

Question. The fiscal year 2006 congressional justification shows that $1 million will be spent on "Purchases from Government Accounts" and $19 million for fiscal year 2006. In response to reprogramming questions, IAIP adjusted the number for "Purchases from Government Accounts" to $20.2 million. Provide a detailed chart on what the $20.2 million will buy in fiscal year 2005 and what the $19 million will buy in fiscal year 2006.

Answer. In fiscal year 2005, the reprogramming of $20.2 million into "Purchases from Government Accounts" includes funding for facilities, Project Management Office, and IT costs. In fiscal year 2006, the $19 million in "Purchases from Government Accounts" will fund the Homeland Secure Data Network (HSDN).

Fiscal year 2005:	
Homeland Secure Data Network	$7,500,000
Shared Services	2,000,000
Facilities	4,500,000
WCF Contribution	7,700,000
IT NCR ops	500,000
Total	22,200,000
Fiscal year 2006: Homeland Secure Data Network	19,400,000

Question. Explain the large increases in fiscal year 2006 for equipment and land and structures.

Answer. The $38 million funding request does not support the design and construction phases of facilities projects. Department Operations requests funds for the facilities design, basic tenant improvements (construction/renovation), physical security upgrades, and emergency power requirements for facilities IAIP will occupy at the Nebraska Avenue Complex (NAC). The IAIP facilities funding is requested to support the costs of occupying facilities, both on and off the NAC, once they are ready, including fit out costs such as furniture, computers and other Information Technology (IT), and the operations and maintenance costs (rent, security, IT support) associated with occupied facilities. Specifically, the operations and maintenance portion of the IAIP facilities funding covers electric costs for additional air conditioning required due to the technology requirements in IAIP spaces (HSOC and server requirements), maintenance for the secure, up to date unclassified and classified Local Area Networks, IT desktop services, as well as required janitorial services. The tenant improvement portion of this funding covers the mentioned fit out costs and ensures facilities capable of meeting both the classified and unclassified space and technology requirements in recognition of the fact that IAIP is an IT and security intensive tenant. These costs include IT infrastructure and cabling, IT equipment, security, IT certification and accreditation, furniture, data migration and relocation costs. The request does not pertain to land, as IAIP is a tenant in GSA-controlled facilities.

CONTRACT EMPLOYEES

Question. In response to fiscal year 2005 reprogramming inquiries, IAIP reported that there are 564 contractors supporting the program function of IAIP, 138 of which are funded through the Management & Administration account and 426 through the Assessments and Evaluations Account.

Of the 426 in the A&E account, what is the distribution of contract support by portfolio?

Answer. Please see chart below.

Account	Contract support
Management & Administration	138
Assessments and Evaluations	426
Homeland Security Operations Center	32
Critical Infrastructure Outreach and Partnerships	74
Cyber Security	78
NS/EP Telecommunications	32
National Infrastructure Simulation and Analysis Center; Protective Actions; Critical Infrastructure; Identification and Evaluation; Biosurveillance	24
Threat Determination and Assessment; Evaluations and Studies; Infrastructure Vulnerability and Risk Assessment	186
Total	564

Question. What makes these positions not inherently governmental positions?

Answer. The support personnel listed against the programs are performing services consistent with Appendix B to Office of Federal Procurement Policy (OFPP) policy letter 92–1. On-site contractor personnel only perform support functions to IAIP and do not perform any activities that are considered inherently governmental. IAIP is currently covering significant portions of the workload associated with open authorized FTE positions (which are inherently governmental) through significant workload sharing of on-board FTE and use of contractors to support non inherently governmental functions of those same FTEs. The mix of contractor support staff will change as programs progress and as new tasks are levied, and workloads will redistribute to more logical and efficient workflows as FTEs come on-board. Although the current work flow arrangements are difficult, they are working due to the dedication and professionalism of the current FTE workforce. IAIP is aware of its responsibilities under the FAIR Act (A–76) and we annually review functions for inherently governmental versus commercial activities.

ASSESSMENTS AND EVALUATIONS

Question. The budget request shows—$137.404 million in Adjustments to Base. For each adjustment on page 76 of the congressional justification for IAIP, explain the reduction or increase.

Answer. Please note that all dollars are in thousands.

CRITICAL INFRASTRUCTURE IDENTIFICATION AND EVALUATION

Description	Adjustment
A decrease of $4,789 is due in part to contractor savings created by the increased number of FTE positions for Field Security Detachments. Additionally, further savings are garnered by the joint funding of Protective Security Task Forces (PSTFs) between Critical Infrastructure Identification and Evaluation (CIIE) and Public Actions (PA). There are elements of the PSTF program that align with CIIE such as the identification of critical infrastructure and the CI/KR expertise of the PSTF team members. However, the overarching emphasis of the PSTF mission is the implementation of protective measures at high priority CI/KR in light of emerging threats. In fiscal year 2006 the program will be funded jointly between CIIE and PA, but the entire program will be transitioned to PA in fiscal year 2007. This is an attempt of IP to better align our programs with the budget structure	($4,789)
A decrease of $899 will be transferred to S&T to support Supervisory Control and Data Acquisition Testing within Cyber Security, responsible for securing the U.S. industrial systems that have become increasingly dependent on powerful, electronic communications tools, the internet, and supervisory control and data acquisition (SCADA) systems	(899)
Total Adjustments to Base	(5,688)

NATIONAL INFRASTRUCTURE SIMULATION AND ANALYSIS CENTER ADJUSTMENTS TO BASE

Description	Adjustment
Travel, includes all costs of transportation of persons, subsistence of travelers, and incidental travel expenses in accordance with Federal travel regulations. In fiscal year 2004 travel for Headquarters personnel was funded from M&A, but has been transferred to A&E for fiscal year 2005 and fiscal year 2006	($5)
Advisory and Assistance Services; the fiscal year 2006 request includes decreases due to decreases in program advisory services and transfers of shared service expenses from A&E back to M&A	(3,995)
Total Adjustments to Base	(4,000)

BIOSURVEILLANCE ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$147
Total Adjustments to Base	147

PROTECTIVE ACTIONS ADJUSTMENTS TO BASE

Description	Adjustment
In fiscal year 2006, the PA program is reduced by $53,000 to establish the new TIP program administered by the SLGCP. TIP grants will be used by state/local/territorial/tribal entities to procure goods and services determined necessary by IAIP's BZPP process. Previously, these goods and services which reduce the vulnerability to terrorist threats around certain high vulnerability critical infrastructures and key assets within the state/local/tribal jurisdiction were funded by assistance from IAIP. The TIP program will also result in a $3,000 savings in program consultation support costs	($53,000)
A decrease of $41,500 for Emerging Pilot Projects and Technology Application Pilots saving initiative	
Technology pilots will be a cooperative effort with S&T for the development of new technologies for protective measures. This effort is funded within S&T	
Emerging Pilot Projects has evolved into the Protective Measures Demonstration Pilots project which takes advantage of innovative uses of existing protective methods and commercially available equipment and technology to enhance the security of CI/KA	
A pilot project would take technology already developed for a specific use and apply it to fill gaps in protective security and evaluate the effectiveness and benefits in ''real life'' or field environments as they relate to IP objectives and priorities. Protective Security Pilots are developed from gaps and protection shortfalls identified in interdependency analysis and consequence of attack analysis as directed by the NIPP, and also from BZPPs, SAVs, and needs identified by Sector Specific Agencies. Pilots are meant to demonstrate solutions for vulnerabilities that cross sectors and stakeholders. Once the means of mitigating the vulnerability is established and proven, the solution is disseminated to all entities that have similar vulnerabilities so that the strategies can be integrated in their respective risk management strategies	
IP is the Sector Specific Agency for 3 sectors (chemical, nuclear, and commercial assets) and is also responsible for cross-sector protection as detailed in the National Infrastructure Protection Plan. IP is responsible for increasing the general level of protection for CI/KR sites absent of specific threat and is also responsible for addressing specific threat events. PSD's intention in fiscal year 2006 is to address the most critical vulnerabilities identified by vulnerability assessments and BZPPs in fiscal year 2005 within the sectors that IP is directly responsible for, including chemical, nuclear and commercial sectors. Other individual sectors and cross-sector vulnerabilities will also be addressed with the demonstration of pilot protective measures based on intelligence and threat information. As directed by the National Infrastructure Protection Plan (NIPP) and HSPD–7, demonstration pilots are also taken on by PSD to mitigate specific vulnerabilities across sectors as the dynamic threat environment changes	(41,500)
A Decrease of $9,800,000 for Regional Protective Actions	
Pilot programs to establish regional centers for use by local law enforcement entities will not be continued in fiscal year 2006. The performance impact will be negligible as PSD will maintain close contact with local police and protective security agencies through the use of the outreach program, training programs, Site Assistance Visits, the BZPP program and visits by Protective Security Advisors and other DHS personnel. DHS also conducts seminars and conferences in order to maintain contact with State and local agencies. PSD has developed close working relationships with local police agencies and will continue to foster and maintain these relationships in the future	(9,800)
Technical Adjustments	4,052

PROTECTIVE ACTIONS ADJUSTMENTS TO BASE—Continued

Description	Adjustment
Total Adjustments to Base	(100,248)

CRITICAL INFRASTRUCTURE OUTREACH AND PARTNERSHIPS ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$885
The cost of maintaining the data center which was funded in fiscal year 2005, in the CIOP program, and initiated under the direction of the Department's CIO is not requested in fiscal year 2006	(35,000)
A $13,800 reduction in CIOP results from a restructuring and completion of analytical tasks, institutionalization of partnership relationships, and implementation of management efficiencies	(13,800)
Total Adjustments to Base	(47,915)

CYBER SECURITY ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$969
Total Adjustments to Base	969

NS/EP TELECOMMUNICATIONS ADJUSTMENTS TO BASE

Description	Adjustment
Advisory and assistance services includes services to support Executive Order 12472, which provides authority for the National Communications System (NCS) to initiate telecommunications service priority programs such as Wireless Priority Service (WPS) and Government Emergency Telecommunications Service (GETS). GETS and WPS are essential telecommunications services to support restoration and recovery following catastrophic events	$1,807
Travel	57
Technical Adjustments	14
Total Adjustments to Base	1,878

THREAT DETERMINATION AND ASSESSMENT ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	($2,043)
Total Adjustments to Base	(2,043)

INFRASTRUCTURE VULNERABILITIES & RISK ASSESSMENTS ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	$3,267
Total Adjustments to Base	3,267

COMPETITIVE ANALYSIS AND EVALUATION ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	($4,000)
Total Adjustments to Base	(4,000)

EVALUATIONS AND STUDIES ADJUSTMENTS TO BASE

Description	Adjustment
Information can be provided under separate cover upon request	$20,139
Total Adjustments to Base	20,139

HOMELAND SECURITY OPERATIONS CENTER ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	($192)
Total Adjustments to Base	(192)

INFORMATION SHARING AND COLLABORATION ADJUSTMENTS TO BASE

Description	Adjustment
Technical Adjustments	$282
Total Adjustments to Base	282

Question. The budget proposes a decrease of $41.5 million for Emerging Pilot Projects and Technology Application Projects with the understanding that "this effort is funded within S&T." There is no budget transfer into S&T for this purpose. Is this just a simple reduction in this area?

Answer. The Emerging Pilot Projects and Technology Application Projects are designed to review existing technologies and help get appropriate protective measures in the field in a usable manner. These pilots and projects identify commercially available or emerging technologies and determine if they can be successfully used to eliminate existing vulnerabilities in a real-world situation. These projects will allow DHS to expand the potential protective measures that can be deployed and to fill existing identified operational gaps. The Technology Application Projects identify commercially available technology and determine if the technology can be applied in the field to fill real needs. The Emerging pilots are required to ensure that any new technology is deployed to the field with appropriate methods and restrictions to allow the state, local, or commercial operators to successfully implement the new technologies. Aspects for successfully technology deployment require: pilots to determine the usefulness of a technology under various conditions; personnel training for deployment and effective use; monitoring methods or personnel required; required response time; technology calibration information; maintenance cycle and manuals, etc.

NOAA WEATHER RADIOS

Question. Virtually none of the funding appropriated for NOAA radios as been obligated by IAIP. Why does this funding remain unobligated?

Answer. IAIP has obligated the procurement and shipment of NOAA "All Hazard" radios to schools across the country. Specifically, a $500,000 pilot program has been funded to disseminate these radios to all the K–12 public schools in certain UASI cities and two rural states. The radios will arrive in September, which coincides with the start of the school year and National Preparedness Month. These radios regularly disseminate weather related information and can now broadcast official DHS alert and warning information. (DHS/IAIP and Commerce/NOAA entered into a MOA in 2004 that provides for DHS message dissemination over NOAA's All Hazard Radio and also over FEMA's local Emergency Alert System.) IAIP, NOAA, Department of Education, DHS Citizen Corps, DHS Procurement, DHS Grants Office, and other DHS entities have been in regular contact regarding this effort for over a year. After lessons have been learned from this initial pilot, additional IAIP alert and warning funds ($1.5 million) will be used for radio procurement for other schools across the country. This $2 million obligation for the radios and the $18 million transferred to FEMA for program management of other alert and warning projects represent all IAIP funding to improve alert and warning for the general public.

VIOLATING THE DHS APPROPRIATIONS ACT

Question. Congress and this Committee take very seriously the constitutional powers bestowed on the legislative branch to enact laws. Article I, Section 9, Clause 7 States that "No money shall be drawn from the Treasury but in Consequence of Appropriations made by law."

Since the beginning of fiscal year 2005, the Department, on several occasions, has violated legislative provisions set forth in the fiscal year 2005 Homeland Security Act. For example, Section 503 of the Act sets strict reprogramming and transfer guidelines restricting the ability of the Department to reallocate appropriated dollars from one program to another without congressional notification. In fiscal year 2005, DHS has violated that provision on more than one occasion. In one instance, DHS stood up a brand new office, called the Domestic Nuclear Detection Office, which has been reporting directly to the Secretary. The start-up costs for this office were taken from funds appropriated to the Under Secretary for Science and Technology. Within the Information Analysis and Infrastructure Protection Office, the Department reallocated funding from an appropriation that pays salaries to its employees to start a new program called Information Sharing and Collaboration. Section 507 of the fiscal year 2005 Act requires DHS to notify Congress on any contract or grant in excess of $1 million 3 business days before it is announced. This provision is an important tool for Congress to keep track of the vast amount of contract and grant funding appropriated to the Department. On several occasions, the Committee has become aware of grants or contracts through the press after the award had been made and without a notification to Congress. In addition, the S&T Directorate spends the majority of its $1 billion annual appropriation on R&D contracts and grants. Through January 31 of this year, the S&T Directorate expended nearly $120 million, yet the Committee has received only 1 grant notifications and 1 contract notification.

Mr. Secretary, I don't expect that you were apprised of these violations nor will you be able to comment on them today. My questions is however, will you look into this pattern of negligence and develop a plan within your office to ensure that the Department will follow the letter of the law as enacted by the U.S. Congress and signed by the President of the United States? As part of your transition review, will you develop a plan to avoid other violations similar to the examples I described?

Answer. The Department takes seriously its responsibility to adhere to the reporting requirements referred to in this question. One of the key imperatives that will drive this Department is to improve DHS' stewardship, particularly with respect to financial management. Likewise, improving communications with Congress, including the timely provision of information such as reports and reprogrammings are important, and will be improved. The Department has already put in place new mechanisms to better track and more aggressively manage reports assigned to DHS by Congress. DHS considers this an important priority and is dedicating significant focus and attention toward ensuring reports are sent to Congress in a timely manner. With respect to the DNDO, the Department provided a reorganization notification and a reprogramming notification, and withheld spending resources for any DNDO activities, including the setting up a DNDO, during the required waiting period. Congress repeated this message in its action on the supplemental in May, and the Department has abided by the requirements and deadlines in that bill and report.

QUESTIONS SUBMITTED BY SENATOR PATRICK J. LEAHY

IMMIGRATION AND CUSTOMS ENFORCEMENT

Question. Immigration and Customs Enforcement (ICE) has been plagued by budget problems basically since the creation of your department. ICE has had a hiring freeze in place since last year and it is unclear when it will be lifted, and only a significant reprogramming request allows it to balance its books for the current fiscal year. Of course, these funding problems are occurring while members of Congress from both parties have emphasized the importance of enforcing our immigration laws in the interior.

How will you ensure that ICE has the funding it needs to perform its mission?

Answer. I am committed to ensuring that ICE has the funding it needs to perform its mission. The fiscal year 2006 President's Budget, which includes $205 million to address base requirements within the agency, along with fiscal year 2005 supplemental funding, will assure that ICE has the necessary funding.

Question. Does the Administration's fiscal year 2006 request provide sufficient funds to avoid another large reprogramming request next year?

Answer. The fiscal year 2006 request provides sufficient funds to avoid another large reprogramming request in fiscal year 2006.

ALL-STATE MINUMUM

Question. I was disappointed that President Bush' proposed budget for fiscal year 2006 reduces from 0.75 percent to 0.25 percent the all-state minimum formula, which I authored, in applying it to the programs under the State Homeland Security Grant Program. This formula assures that each State receives a minimum of 0.75 percent of those grants to help support their first responders' basic preparedness needs.

Not only would this change result in the loss of millions in homeland security funding for the fire, police and rescue departments in small- and many medium-sized states, but also deal a crippling blow to their efforts to build and sustain their terrorism preparedness.

Mr. Secretary, does this Administration want to shortchange rural states, rolling back the hard-won progress we have begun to make in homeland security by slashing the protections provided to us by the all-state minimum?

Answer. For fiscal year 2006, DHS proposes to redesign the homeland security funding process to award State HSGP funds based on an evaluation of risk and needs. The intent of this approach is to change the way DHS invests its limited homeland security resources in order to achieve the greatest return on investment for our nation's homeland security. This is consistent with recommendations from the 9/11 Commission, which contends that Federal homeland security assistance should supplement State and local resources based on the risks or vulnerabilities that merit additional support. As proposed, fiscal year 2006 awards will be based on a relative evaluation of risk and application-based review of need with no State receiving less than 0.25 percent. DHS will consider risk factors such as threat, presence of critical infrastructure, vulnerability, population and population density, international borders, and ports of entry in making final award determinations. In the consideration of need, DHS will undertake an assessment with the States and territories to identify their capabilities and gaps consistent with the capabilities and tasks identified under Homeland Security Presidential Directive-8. In addition, at least 20 percent of funds awarded will be dedicated to support law enforcement terrorism prevention activities. Overall, this approach will result in the achievement of the highest possible readiness to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy.

Question. Mr. Secretary, would you agree that homeland security is a national responsibility shared by all states, regardless of size?

Answer. Yes, DHS strongly believes that homeland security is not only a Federal responsibility, but it requires collective national and even international action. The protection of our citizens, our critical infrastructure, our businesses, and our communities is a shared responsibility, requiring Federal, state, local, international, and private sector partnerships. The partnership required to protect the homeland involves sharing information as well as responsibility. For that reason, allocation of State and local grant funding should reflect the best available data and analysis of the threats, risks, and unmet needs—not static formulas.

Question. Mr. Secretary, do you agree that each State has basic terrorism preparedness needs and, therefore, a minimum amount of domestic terrorism preparedness funds is appropriate for each state?

Answer. The President's Request proposes a 0.25 percent allocation to be provided to each State as a supplement to State and local resources allocated to domestic preparedness. DHS resources should be used to enhance basic levels of preparedness and not to supplant State and local responsibilities. In addition, the Department believes that States and urban areas should focus on a set of collective capabilities needed to prevent, protect against, respond to, or recover from a terrorist attack or catastrophic event. Through the newly-developed Interim National Preparedness Goal and the accompanying National Planning Scenarios and Target Capabilities List, the Nation will begin to implement a coordinated approach to national preparedness, utilizing a risk-based and regional methodology.

Question. If you do not support applying the 0.75 percent minimum to the State Formula Grants Program, what compromise between 0.75 percent and 0.25 percent for the distribution of funds would you support?

Answer. The DHS proposal to reduce the minimum State allocation from 0.75 percent to 0.25 percent is based on the redesign of the homeland security program to support a risk and need-based approach to funding. Factors such as threat, presence of critical infrastructure, vulnerability, population, borders, and POEs will be used

to make final award determinations. An increase in the base percentage allocation would result in a reduction in resources available for those States with the greatest risk and needs. Therefore, DHS believes that raising the minimum allocation is not conducive to maintaining maximum readiness.

FIRST RESPONDERS (GENERAL)

Question. President Bush often says that he wants to ensure that our State and local first responders receive the resources necessary to do the job the American public expects them to do. I find that hard to believe, though, when I read that he proposes a $455 million overall cut in funds for State Homeland Security Grant Program, Law Enforcement Terrorism Prevention Program, Emergency Management Performance Grants and other programs SLGCP Office that directly benefit police, fire and medical rescue units. The Administration argues this is justified because it does not believe those funds are "targeted" to homeland security capabilities.

I believe, however, that the current Administration has failed to make first responders a high enough priority by consistently underfunding homeland security efforts of every state.

The Hart-Rudman Terrorism Task Force Report argued that our Nation will fall approximately $98.4 billion short of meeting critical emergency responder needs through this decade's end if current funding levels are maintained. Clearly, the domestic preparedness funds available are still not enough to protect from, prepare for and respond to future domestic terrorist attacks anywhere on American soil.

Would you agree, Mr. Secretary, that to be truly protected from, prepared for and able to respond to terrorist attacks we must look to increase the funds to our Nation's State and local first responders, rather than decrease them, as proposed by the President?

Answer. The President's fiscal year 2006 Budget request includes $3.6 billion for SLGCP to continue our strong commitment and support to the nation's emergency prevention and response community. Of this amount, $1.02 billion is for the State HSGP, which has been significantly redesigned to award funds based on risk and need, while aligning with national priorities. An additional $1.02 billion is for the continuance of the UASI, which targets funds to the nation's highest risk urban areas. Further, the President's request provides $600 million for a new TIP Program to supplement state, local, and private sector infrastructure protection efforts based on critical vulnerabilities. The fiscal year 2006 request also includes a strong commitment to our nation's fire service by providing $500 million for the Assistance to Firefighters Grant Program. The request includes $50 million the CCP and $170 million for the EMPG. For continuation of our commitment to training our nation's first responders, the request includes $94.3 million for SLGCP's State and Local Training Program. The request also includes $59 million for the National Exercise Program, which includes support for State and local exercises and for the National Top Officials exercise series. Finally, the request includes $10.6 million for technical assistance initiatives for State and local agencies and $14.3 million for program evaluation and assessments. Between fiscal year 2002 and fiscal year 2004 the SLGCP awarded homeland security grants totaling $6.1 billion. In fiscal year 2005, SLGCP anticipates awarding an additional $3.64 billion in grants. We believe, at this point, that funding provided to our nation's first responders has been sufficient to address their critical needs.

BORDER PATROL

Question. The intelligence reform bill Congress passed and the President signed last December mandated an increase of 2,000 Border Patrol agents in fiscal year 2006, with an increase of 400 agents at the Northern Border. The President's budget for DHS would pay for an increase of slightly more than 200 agents, or about 10 percent of what Congress called for. None of these new agents would be deployed on our Northern Border.

Why does the Administration believe that an increase of about 200 agents is sufficient to secure our borders?

Answer. Following the terrorist attacks of September 11, 2001, the CBP Border Patrol has accelerated its efforts in increasing its enforcement presence along the northern border to achieve the definitive goal of operational control, and the number of agents allowing the northern border more than tripled. DHS is completing work on comprehensive immigration reform, which calls for additional new hires. We have supported additional agents in fiscal year 2006 consistent with both House and Senate appropriation marks for CBP hiring.

Question. Would additional agents beyond the number proposed by the President be useful to the Department's efforts to prevent illegal entry into the United States?

Answer. The Department appreciates the 500 additional agents funded in the Emergency Supplemental. As noted above, the Department is in the midst of a systems-level review of its border control architecture.

ICE/CBP MERGER

Question. As you know, there has been substantial discussion in recent months about a possible merger of Immigration and Customs Enforcement with Customs and Border Patrol. Do you support such a merger?

Answer. I do not support a merger at this time. ICE and CBP were formed just two and a half years ago and the transition to the current structure has been challenging. I am concerned about embarking on yet another far reaching transition affecting these organizations. Most importantly, however, it is too soon to say that the current structure will not effectively serve our border missions. As we move forward with comprehensive reforms and improvement to our border security and immigration system, I am confident that both ICE and CBP can operate in an effectively coordinated manner without being merged.

QUESTIONS SUBMITTED BY SENATOR PATTY MURRAY

PORT SECURITY

Question. Mr. Secretary, one of my greatest concerns—as a Senator from a State that depends on its seaports for its livelihood—is that we have a cohesive port security plan that protects our communities and our economy from potential threats.

Yet the Administration's budget request again seeks to eliminate the Port Security Grant program.

Mr. Secretary, as I've mentioned before, the Coast Guard Commandant testified that it would take more than $7 billion to implement the Maritime Transportation Security Act. To date, we have provided a little more than $500 million toward this $7 billion—most of which was not requested by the Administration. Mr. Secretary, for the past 2 years, nearly $1 billion in port security grant requests came to DHS annually. And, the American Association of Ports Authorities has estimated that there is a need of at least $400 million to help secure our port facilities this year. From our discussions, I know that securing our ports is a priority for you. And, again, I realize you did not draft this budget—but you've been sent here to defend it.

I must ask—is this a budget game the Administration is playing, or does the White House discount all of the intelligence reports that tell us our ports are a significant risk?

Answer. Enhancing the security of the nation's critical infrastructure, especially its ports, continues to remain a high priority for the Department. For fiscal year 2006, DHS is proposing to consolidate the Port Security, Rail/Transit Security, Buffer Zone Protection (BZP) Program and Trucking Industry Security grant programs into the single TIP Program. Combined resources for the fiscal year 2005 distinct programs totaled $315 million. The DHS fiscal year 2006 request for the TIP Program is $600 million, almost double the amount of fiscal year 2005 available resources for the distinct fiscal year 2005 programs. With that being said, funds provided through TIP will directly enhance the ability of the owners and operators of key port assets and transit systems to prevent and respond to large scale incidents. In fiscal year 2005, DHS shifted to a more risk-based allocation of funding across sectors, as well as integration of these programs with regional homeland security planning efforts, such as those required by the UASI. The fiscal year 2005 program also considers intelligence and threat data to set specific security enhancement priorities. The fiscal year 2006 TIP Program will continue to build on these enhancements by shifting to a discretionary approach for all program elements, allowing DHS to better supplement state, local and private sector infrastructure based on risk. Additional priorities for the fiscal year 2006 program include further enhancing the linkages between critical infrastructure protection and regional planning efforts, and a continued emphasis on security investment at ports and transit agencies based on relevant intelligence and threat data. In the end, this will result in a more agile and responsive program based on risk.

CARGO SECURITY

Question. Mr. Secretary, I know we both agree the agencies involved in securing these seaports are doing an admirable job—they are working through a difficult problem.

Yet, they aren't being given the proper tools, resources, and guidance to knit together a coordinated port security regime for our nation.

Last year, I added language into the fiscal year 2005 Committee Report that directed the Under Secretary of Border and Transportation Security to develop a plan to create that coordinated approach to port security. That report was due—quote—no later than February 8, 2005. Yet, we have not received that report. Unfortunately, the message that the Administration has sent is that the White House is not willing to take the responsibility for developing and implementing such a plan.

Mr. Secretary, I've discussed this issue at great length with you, Deputy Secretary Jackson, Commissioner Bonner, your predecessors—anyone who might listen.

I've talked about legislation and additional funding but all we have seen from the Administration is a directive that appointed a new Commission to study the issue.

Mr. Secretary, I know we agree this is an issue of importance. What do you believe we need to do—how can we help you come up with a coordinated approach to secure our ports, the cargo moving through them and the people who work and live near them?

Answer. The report was submitted on June 8, 2005.

Maritime and supply chain security remain priorities for DHS. When the President signed HSPD–13/NSPD 41 in December 2005, he indicated the Administration's commitment to addressing port security as part of the greater maritime system. In this Directive, DHS and DOD were directed by the President to develop a strategy for securing the Maritime domain, including a variety of issues related to port and cargo security. DHS is actively working with DOD and other Federal partners to meet this goal.

In addition, I am reviewing the status of DHS's cargo security efforts, how they can be further strengthened and how we can further transform the system to ensure the United States security and economic needs are met.

HAMMER TRAINING

Question. Mr. Secretary, as you might be aware, Washington State is home to the The Volpentest Hazardous Materials and Emergency Response Training and Education Center—we know it as HAMMER.

This is a state-of-the-art, Department of Energy facility with expertise in threats posed by chemical, radiological, and biological agents, hazardous materials, and weapons of mass destruction. HAMMER specializing in hands-on training for first responders but the Department has not designated this facility a regional training center. Instead, first responders from throughout the Northwest have to use their local budget—or DHS funding—to travel to facilities around the country for the training they could receive close to home. Under the fiscal year 1999 Defense Authorization Act, the Secretary of Energy was specifically authorized to enter into partnership arrangements with to share the facilities at HAMMER with Federal agencies. Under the Homeland Security Act of 2002, you are authorized to enter into joint sponsorship arrangements with the Secretary of Energy to use DOE sites to carry out the missions of the Department of Homeland Security. Mr. Secretary, we have a great facility at HAMMER and I encourage you to come personally, or send your staff out to visit. I know that when you see their capabilities, you will agree that using HAMMER as a designated training center would be a benefit to both the first responder community throughout the Northwest—and DHS itself.

Will you visit HAMMER and consider adding it as a member of the National Domestic Preparedness Consortium?

Answer. The NDPC was chosen based on each member's expertise in first response training. At present, plans to expand DHS' training network are extremely limited, and more than likely will not include the establishment of additional consortium members or residential training facilities. Under the provisions of the Department of Homeland Security's fiscal year 2004 Appropriations Act (Public Law 108–90), ODP received funds for a limited "competitive training grants" program to supplement training efforts provided through the National Domestic Preparedness Consortium. The Competitive Training Grant Program (CTGP) was developed to facilitate national scale training programs, and the fiscal year 2004 program funded 14 training sites. Currently, the Department is undergoing its evaluation process for fiscal year 2005 CTGP applicants. In addition, enhancing existing training programs is an eligible use of other SLGCP grant funds. The Department encourages HAMMER to explore the use of other DHS grants as a potential source of Federal funding in the future.

NORTHERN BORDER SECURITY

Question. Mr. Secretary, the President's budget request only includes funding for 210 of the 2,000 new border agents called for by the Intelligence Reform Act that was signed into law last December.

We currently have about 11,000 Border Patrol agents and 90 percent of them are stationed on the southern border. We have a major security issues at our northern border—ranging from drug trafficking to the apprehension of potential terrorists—and they aren't being addressed.

What kind of message is this sending to our border communities? Is stepping up this security going to be a priority for you?

Answer. Following the terrorist attacks of September 11, 2001, the CBP Border Patrol has accelerated its efforts in increasing its enforcement presence along the Northern Border to achieve the definitive goal of operational control, and the number of agents allowing the Northern Border more than tripled. This accelerated and focused effort has clearly provided the Nation with a more secure Northern Border. Moreover, Emergency Supplemental Legislation and President Bush's fiscal year 2006 Budget call for the hiring of an additional 710 agents by the end of fiscal year 2006, and CBP is taking aggressive steps to recruit, hire and train candidates to fill these spots. The hiring of these new agents comes in addition to the standard attrition hires that supplement the several hundred agents who retire, transfer, or leave for medical reasons over the course of a year. New agent positions will be allocated based on risk-based priorities. That said, effective control of the border—Northern or Southern—requires a more comprehensive approach than simply adding more agents.

DHS is accordingly in the midst of a systems-level review of its border control architecture to identify the right mix of personnel, technology and infrastructure to help achieve effective control of the border. DHS will identify a program manager to oversee the development of a specific set of border security plans.

NORTHERN BORDER AIR WING

Question. Along those lines, the first Customs Air and Marine Operations Wing was established in Bellingham, WA last summer. I was very happy to be there at the dedication and have worked with Director Stallworth to get the program up and running. The second air wing is in Up-State New York and 3 more are planned. We need to make these a priority—especially with the lack of Border Patrol agents on the Northern Border. They also need to be able to communicate with the local law enforcement. Since that time it has become clear that many local law enforcement jurisdictions don't have compatible radios—our eyes-in-the-sky can't coordinate with the police on the ground. I'm told it would cost about $5 million to run a pilot program.

Do you agree that this is an issue we should deal with? Will you help make this happen?

Answer. Deployment of additional Northern Border airwings will be addressed as part of the CBP Air and Marine program integration review now underway. This review is expected to be completed in the summer of fiscal year 2005.

NORTHER BORDER PROSECUTIONS

Question. Mr. Secretary, because of the increased presence and law enforcement activity on the northern border, incarcerations and prosecutions are up dramatically since September 11. The major border crossing between Seattle and Vancouver, BC is in Blaine—a very small community compared to Detroit and Buffalo—and a very limited local tax base to cover these costs. This community has already seen more than a $3 million increase in prosecution costs simply because they are located on the border. This trend is expected to continue with an expected $4 million in prosecution and incarceration costs in fiscal year 2005. Mr. Secretary, this community needs some special help—they don't have the tax base or population to sustain this and even greater increases.

What can your Department do to help communities like this one?

Answer. DHS has committed significant resources to address the increase in smuggling activity between the United States and Canada, as well as the demonstrated vulnerabilities that exist on the Northern Border. This dedication of enforcement resources has resulted in an increase in arrests, seizures, and prosecutions involving border related criminal activity. Some prosecutions based on DHS enforcement activities have been deferred to the State for prosecution since the violators also fall under State law.

SEATAC AIRPORT

Question. Secretary Chertoff, I am very concerned with the reports that Seattle Tacoma International Airport in Washington State may see a reduction in their Federal security screener force this year. Currently, SeaTac Airport is facing a shortage of approximately 200 FTEs to meet the summer travel season at present staffing levels. Without these additional screeners SeaTac will undoubtedly see repeats of 2002 and 2003 that saw security lines regularly exceeding 1 hour.

Mr. Secretary, I request that you review the situation at SeaTac and work with the local Federal Security Director to ensure that SeaTac's screener staffing level allows the airport and TSA to provide the same level of customer service achieved last year.

Answer. Based on the Screener Staffing Model, SeaTac Airport (SEA) is currently below its required staffing level. TSA is in the process of bringing SEA up to that staffing level. Recruitment of new screeners is underway.

SUBCOMMITTEE RECESS

Senator GREGG. The hearing is recessed.

[Whereupon, at 12:09 p.m., Wednesday, April 20, the subcommittee was recessed, to reconvene to subject to the call of the Chair.]